

An efficient classification in IBE

Provide with an improvement of BB2 to an efficient Commutative Blinding scheme

Rkia Aouinatou¹, Mostafa Belkasmi²

¹ Faculty of Sciences, Mohamed V-Agdal B.P. 1014 Rabat, Morocco

* *Laboratoire de Recherche Informatique et Telecommunication: LRIT*

Email: rkiaaouinatou@yahoo.fr

² ENSIAS: University Mohammed V- Souissi, Rabat, Morocco

Email: belkasmi@ensias.ma

Abstract

Because of the revolution and the success of the technique IBE (Identification Based Encryption) in the recent years. The need is growing to have a standardization to this technology to streamline communication based on it. But this requires a thorough study to extract the strength and weakness of the most recognized cryptosystems. Our first goal in this work is to approach to this standardization, by applying a study which permit to extract the best cryptosystems. As we will see in this work and as Boneh and Boyen said in 2011 (Journal of Cryptology) the BB1 and BB2 are the most efficient schemes in the model selective ID and without random oracle (they are the only schemes traced in this model). This is right as those schemes are secure (under this model), efficient and useful for some applications. Our second goal behind this work is to make an improvement in BB2 to admit a more efficient schemes. We will study the security of our schemes, which is basing on an efficient strong Diffie-Hellman problem compared to BB1 and BB2. More than that our HIBE support s^+ ID-HIBE compared to BBG (Boneh Boyen Goh). Additionally the ID in our scheme will be in Z_p instead of Z_p^* as with BBG. We will cite more clearly all these statements in in this article.

keywords

IBE, competition, RO, SM, sID, BF, SK, BB1, BB2, Water, Gentry, Problem Bilinear of Diffie Hellman, HIBE, BBG, selective ID, $selective^+$ ID, Z_p^* , complexity, security.

1 INTRODUCTION

IBE was proposed by Adi Shamir in 1984 [1] as a solution to the problem of the revocation of the public key and the requirement of the certificate in PKI. In IBE (Identification-Based Encryption) the public key can be represented as an arbitrary string such as an email address. It's corresponding private key is generated by a Private Key Generator (PKG) who authenticate users according to their corresponding identities. This idea was proposed by Shamir only as concept. And we will wait until 2001 at which Dan Boneh and Mathew Fanklin [2] propose an elegant scheme in the Random

Oracle, using the pairing. Their proposition open the door to a more efficient scheme (with pairing), we cite : Boneh-Franklin (BF) [2], Skai-Kasarah (SK) [3] under the model Randoms Oracles, Boneh-Boyen (BB) [4] under the model selective ID, Water [5] and Gentry [6] under Standard Model. These cryptosystems are the great themes of the cryptography IBE, because all the cryptosystems which comming later : [7,8] and others, are just their modified.

After all these proposals several companies have begun working with IBE instead of the PKI. We can cite Voltage Security and Nortech. This seeks to balance the standardization of the communication, which is currently being prepared (already tried by IEEE [9]). But to do it we need a very thorough study because we need to consider many things. In this study we make a comparison between the main cryptosystems we have cited.

The comparison in the IBE has been treated in a lot of papers, for example : Boyen [10] call to the standardization of BB1 (IEEE 1363.3) by showing its benefit. The same author [11] make a comparison between BB1, SK, BF. In [7] Kiltz-Vahl propose two cryptosystems which they have shown their advantage over that of Gentry and Kiltz-Galindo. Note that every time a cryptosystem is invented it begins to describe their advantages over others. Unfortunately all these studies are not conclusive. Because, either they do not take into account all the major cryptosystems, or the numbers of the factors at which the comparison is based are insufficient. In this work we will make a practical comparison between all the proposed cryptosystems, by integrating the most possible factors and proposing a suitable schedule.

Usually the systems networks become more accessible and open, apparently an active adversary (even passive) may not be limited to eavesdropping, but may take a more active role. She can interact with honest parties, she may analyze some older responses, she can try to break some problem of Diffie Hellman used in the target cryptosystem...That's why it is out of habit and within the cadre of standardization, that the security of each cryptosystem will be checked by what is called studies of simulations. Those studies are introduced by [12], they are being done in advance to test the rigidity of a cryptosystem. But all of them require that the identity wishing to be attacked will be asked in the challenge phase. We call this, full domain. In 2003 Canetti et al. [13] proposed a weaker security model, called selective identity IBE (sID-IBE). In this model the adversary must commit ahead of time to the identity it intends to attack. In [14] Sanjit Chatterjee et al have presented an extension of this model at which the adversary is allowed to vary the length of the challenge identity. Which is not allowed in the sID model. Naturally any protocol secure in the s^+ID model is also secure in the s-ID model, but the converse is not necessarily true.

Even if the reduction from selective-ID IBE to fully secure IBE introduces a factor of $N[4]$ (N will be at least 2^{160} to make the problem bilinear rigid) in the security parameters of the system. Boneh and Boyen in 2004 [4] have proposed tow efficient schemes BB1 and BB2 under this model. The first one is in the approach of Commutative Blinding, it is an HIBE scheme based on the DBDHP (Decisional of Bilinear Diffie and Hellman Problem). Until the second is in the Exponent-Inversion approach, it is an IBE based on Dq-BDHIP (Decisional q-Invertible of Bilinear Diffie and Hellman Problem).

As an IBE requires the use of a PKG to generate the private key, so alone PKG is insufficient. Since, it will be a concentration in one. To avoid this the works [15][16] and others are proposed. All them are heavy, because for k authority in hierarchy it necessitate to generate k element in extract and in encrypt, in addition to k product of pairing in decrypt. This cost was reduced by Boneh, Boyen, Goh [17]. In [17] the authors propose a scheme where the ciphertext size and the decryption cost are independent of the hierarchy depth. The ciphertexts is always just three group elements and decryption requires two bilinear map computations. This reduction influence on some application such as Forward HIBE and Broadcast Encryption.

But even the authors in [17] reduce the cost in the syntax of HIBE, their scheme requires that the

identity to be challenged will be in Z_p^* , because they necessitate it in the technique of the study of simulation to remove the master key g^α . This limit the choice of the identities which is a restrict. More than that, their proposal was not familiarized with the notion of s^+ID , and it is proven in [14] that if want to convert s-ID to s^+ID we will make a degradation of h ($h=v \cdot v^+$, v is the length of the identity challenged, and v^+ is the target prefix). This give a more advantage to attack the cryptosystem, as we may have an advantage equal to $h\varepsilon$.

Our second contribution behind this work is : To over come all this. Keeping the syntax of BB2 (noting that BB1 and BB2 are considered until 2011 [18] as an efficient schemes in the sID Model), we will propose a scheme (with a little change in BB2) in the Commutative Blinding approach and which requires only 1 pairing in decrypt contrary to BB1. With the same manner, we will reduce the HIBE following BBG. This reduction, will help us to give a more efficient Forward HIBE and even Broadcast Encryption. By contrast to BBG our result HIBE support s^+ID model and it can project in the Z_p contrary to Z_p^* as with BBG.

Organization

Firstly we will divide our work in tow categories : First goal and second goal.

We begging in the first goal by some preliminaries, section number 2.2 will be reserved to the comparison (in two level : complexity and security). Our final decision will be given in section 2.3. For the second goal we will also staring by some notions, it concerns the functionality of IBE, HIBE and their security, in addition to that we give some preliminaries concerning the problem of Diffie Hellman to be used. We reserve section 3.2 and 3.3 to our proposal for IBE and HIBE respectively, then we test the efficiency of our schemes compared to BB1, BB2 and BBG. In section 3.4 we demonstrate the utility of our scheme for Forward scheme. In the end we give a conclusion.

2 First goal

2.1 Some Preliminaries

Before giving some of these preliminaries, we remember that our first goal about this work is to classify the main cryptosystems. The cryptosystem's which are in competition are : Boneh Franklin, Skai Kasarah, Boneh Boyen (BB1, BB2), Water, Gentry.

2.1.1 Relation of the Problems of Diffie and Hellman

2.1.1-1 Problem Bilinear of Diffie Hellman

Definition 1 : (Bilinear Diffie Hellman Inversion Problem (k-BDHIP) [5]). Let k be an integer, and $x \in Z_q^*$, $P_2 \in G_2^*$, $P_1 = \psi(P_2)$, $\hat{e} : G_1 \times G_2 \longrightarrow G_T$. Given $(P_1, P_2, xP_2, x^2P_2, \dots, x^kP_2)$, compute $\hat{e}(P_1, P_2)^{\frac{1}{x}}$ is difficult.

Definition 2 :New Problem : SiE-BDHP (Simple Exponent Bilinear Diffie Hellman Problem). We express it for the first time in the literature : Let k be an integer, (P_1, P_2) in $G_1 \times G_1$, $x \in Z_q$, given $P_0, xP_1, xP_2, xP_3, xP_4, \dots, xP_k$. Compute xP_0 is difficult

Definition 3 : (Bilinear CAA1 (k-BCAA1) [19]). Let k be an integer, and $x \in Z_q^*$, $P_2 \in G_2^*$, $P_1 = \psi(P_2)$, $\hat{e} : G_1 \times G_2 \longrightarrow G_T$. Given $(P_1, P_2, xP_2, h_0, (h_1, \frac{1}{h_1+x}P_2), \dots, (h_k, \frac{1}{h_k+x}P_2))$, with $h_i \in Z_q$, for $0 < i < k$ are distinct. Calculate $\hat{e}(P_1, P_2)^{\frac{1}{(x+h_0)}}$ is difficult.

Definition 4 : (Bilinear Diffie-Hellman Problem BDHP [2]). Let G_1, G_2 two rings with prime order q . Let $\hat{e} : G_1 \times G_2 \longrightarrow G_T$ be an application admissible and bilinear and let P be a

generator of G_1 . The BDHP in $\langle G_1, G_2, \hat{e} \rangle$ is so : Given $\langle P, aP, bP, cP \rangle$ for $a, b, c \in \mathbb{Z}_q$. Calculate $\hat{e}(P, P)^{abc} \in G_2$ is difficult.

Definition 5 : (Augmented Bilinear Diffie-Hellman Exponent Assumption q-ABDHP [6]). Let k be an integer, and $x \in \mathbb{Z}_q^*$, $P_2 \in G_2^*$, $P_1 = \psi(P_2)$, $\hat{e} : G_1 \times G_2 \rightarrow G_T$, given $(P_1, x^{k+2}P_1, P_2, xP_2, x^2P_2, \dots, x^{2k}P_2)$. Calculate $\hat{e}(P_1, P_2)^{x^{k+1}}$ is difficult.

Definition 6 : Problem calculator of Diffie Hellman : CDHP. Given P, aP, bP can we find or rather calculate abP ?

Definition 7 : Problem Decisional of Diffie Hellman

Given P, aP, bP, cP can we say that $abP = cP$? But this problem can be solved in polynomial time after using the pairing, for example if we prove that : $e(P, cP) = e(aP, bP)$ so $abP = cP$. This strategy is valid to others problems for example the q-BDHIP and q-ABDHE

2.1.1-2 Relation

Firstly, we discuss and show the relationship between the problems of Bilinear Diffie Hellman, with which the studies of simulations of the cryptosystems in competition are based. Study the classification of these problems is useful, because the rigidity of these studies is based on them. So we have :

$$\begin{aligned} \text{BDHP (1)} &\longrightarrow \text{BDHIP (2)} \\ \text{BDHP (1)} &\longrightarrow \text{ABDHP (2)} \\ \text{BDHP (1)} &\longrightarrow \text{DBDHP (3)} \\ \text{BDHIP (2)} &\longrightarrow \text{DBDHIP (4)} \\ \text{ABDHP (2)} &\longrightarrow \text{DABDHP (4)} \end{aligned}$$

Relation and Classification

We have classed DBDHP in class 3 compared with BDHIP and ABDHP, because, it can be calculated in polynomial time using the Pairing. And we give the same rank to ABDHP and BDHIP, since until present, there is no relationship which can link these two problems, all we can say is that they belong to the same category (queries in the form exponentiations).

As long as, DBDHP has a rank before that of DABDHP and DBDHIP, because, (ignoring that $\text{BDHP} \longrightarrow \text{ABDHP}$ and BDHIP) the BDHP is rigid than BDHIP and ABDHP. Since theses latter have complexity $O(\sqrt[3]{q})$ after [20]. So, the DBDHP is also rigid than DABDHP and DBDHIP. Recall that : BF (BDHP), SK (BDHIP), BB1 (BDHP) BB2 (DBDHIP), Water (DBDHP), Gentry (DABDHP).

In the other part, IBE has been built to serve a broad category of a persons (in a classified area), using a single system of parameter. The only things that is change is the private keys, which are generated from a single master key for all the applications. So it may be that there exist enemies among the customers (the domains), who are agree to break the Master key of the authority from the syntax of the private key. So the success of this study related to the syntax of each private key. The private key of the cryptosystems in competition are in the form : BF has the form SiE BDHP (sQ_{ID_i} for each i varied), that's of SK has the form BCAA1 ($\frac{1}{s+H(ID_i)}$). BB1 is based on PDL, as so not to extract α, β, ϖ from respectively $\alpha P_{pub}, \beta P_{pub}, \omega P_{pub}$. Also, we wouldn't calculate P_{prive} from rP_{prive} , since, if this will be easy, it will be easy also to associate a random r to $(\alpha H(ID) + \beta)P_{prive} + \omega P_{prive}$. So, breaking easily the cryptosystem as we have the division of two Pairing. For BB2 it has the private key following the form BCAA1 ($\frac{1}{s_1+ID_i+s_2r}$). The syntax of the private key of Water is like BB1 based on PDL, as that of Gentry is under the form BCAA1.

As it is generally known the PDL has complexity $O(\sqrt{q})$ and the BCAA1 has $O(\sqrt[3]{q})$ [20], as it is from the category of the Problem Diffie Hellman in form Exponentiations. For the SiE-BDHP we haven't a complexity exact, all we can say is that it is less than PDL and more than BCAA1, since $PDL \rightarrow SiE-BDHP \rightarrow EBDHP \rightarrow BCAA1$ (EBDHP Exponent Bilinear Diffie Hellman Problem [19]). So we have this classification following the rigidity of the private key : BF(2), SK(3), BB1(1), BB2(3), Water(1), Gentry(3)

2.1.2 Random Oracle & Standard Model

Random Oracle : In cryptography, an oracle is a random that answers all queries proposed at random and specific request (for more details we send the interested to [21])

The utilization of the Random Oracle has some dangers, we cite in this article :

The Random Oracle responds with random values and therefore, it will be difficult to precise the suitability of its values with the conditions allowed. More, because of the random values of the Random Oracles which are difficult to adapt, the crypto systems under this model use in their demonstrations an arbitrarily values chosen. Which makes these cryptosystems unclear in their study of simulations (q_H is not related directly to the syntax of the cryptosystem but it is arbitrary). The Random Oracle still has more danger and to knowing it we refer the interested to [22]. By contrast, in the Standard Model, which use any Random Model we are sure about what is happening, as we use the Mathematical formulas. But in the Random Oracle we communicate with a spirit random which hasn't any exact measure.

2.1.3 Studies of Simulations

The studies of simulations are invented by [12], they are being done in advance to test the rigidity of a cryptosystem. And in this article we cite :

CPA : Is the abbreviation of Chosen Plaintext Attack ie during the studies of simulations the opponent has advantage to access to the encrypted of his chosen texts.

CCA : It is an abbreviated of Chosen Ciphertext Attack, and we divide it into two parts : CCA1 and CCA2. During CCA the adversary has advantage of access to the decrypts texts he has chosen. In the CCA1 the opponent is less limited by comparison with CCA2. We must say that the CCA2 is the most powerful among all these attacks.

In 2003 Canetti, Halevi and Katz proposed an alternative strategy in the study of simulation, at which the adversary must commit ahead of time to the challenge identity. And so, the identity to attack must be declared in advance. This early model is referred as selective-identity attack (sID), while the Original Model is called Full-identity scenario (ID). According to [23] the selective ID (sID-CCA/CCP) is less rigid than (ID-CCA/CCP). The ID-CCA is required to merit the Standardization.

2.1.4 Advantage of the Cryptosystem

In this section, we compare the advantage of each cryptosystem in competition. Recall that an advantage is done to learn the skill of an opponent to break a cryptosystem, basing on specifically mathematical probabilities. For our cryptosystems we have :

Adv_{BF} (Advantage of BF) = $\frac{1}{(q_{H3}+q_{H4})q_{H2}} [(\frac{\epsilon}{q_{H2}}(1-\frac{q_E}{q_{H1}})+1)(1-\frac{2}{p})^{q_D}-1] - \frac{3}{6} \sim \frac{\epsilon}{q_{H3}}(1-\frac{2}{p})^{q_D}$; $Adv_{SK} = (\frac{\epsilon}{q_1+1})(1-\frac{2}{p})^{q_D}$. For the two crypto system BB1 and BB2 we utilize a propriety demonstrated by Boneh Boyen [4] which say that :

Let (t, q_S, ϵ) -selective identity secure IBE system (IND-sID-CPA). Suppose E admits N distincts identities. Then E is also a $(t, q_S, N\epsilon)$ -fully secure IBE (IND-ID-CPA). So basing in this propriety

we have : $Adv_{BB1} = \varepsilon \cdot 2^n \cdot \frac{q_H}{(2^n - q_S)}$; $Adv_{BB2} = \varepsilon \cdot 2^n$. As long as following [5] and [6] we extract easily : $Adv_{Water} = \frac{\varepsilon}{32(n+1)q}$; $Adv_{Gentry} = \varepsilon + 4\frac{q_C}{p}$. To compare this advantages we take into consideration : q_S & $q_D < q_H < n \ll p$. So we have : $Adv_{Water} < Adv_{BF} < Adv_{SK} < Adv_{Gentry} < Adv_{BB1} < Adv_{BB2}$. Consequently, Water is the most desirable as it has a very small advantage

2.1.5 Anonymity

Anonymity is a method to distinguish the identity of a person from the ciphertext. This property is more desirable in cryptography, because it limits the activity of an opponent in the beginning. As a result, the opponent will be incapable to know the person addressed in the ciphertext. For our cryptosystems only Boneh Franklin and Gentry are Anonymous

2.1.6 Pairing

A pairing is a bilinear map that takes two points on an elliptic curve and gives an element of the group multiplicative of n-th roots of unity. Among the pairing we cited : Weil, Tate, Ate, η , but in the implementations cryptographic we often use Weil and Tate.

Pairing of Weil

The Weil pairing is defended as follows : $e_r : E[r] \times E[r] \rightarrow \mu_r$ (μ_r is the set of the r^{th} root of the unity) such that : $e_r(P, Q) = \frac{f_{D_Q}(D_P)}{f_{D_P}(D_Q)}$

Pairing of Tate

The Tate pairing is the application :

$$t_r : E(k)[r] \times E(k)/rE(k) \rightarrow k^*/(k^*)^r$$

$(P, Q) \rightarrow t_r(P, Q) = f_{D_P}(D_Q) \text{ modulo } (k^*)^r$. And to have an exact value, it can be defined as follows :

$$t_r(P, Q) = (f_{D_P}(D_Q))^{(q^k - 1)/r}$$

2.1.7 Inverse of two Pairing

The inverse of two pairing is calculate as [24]

$\frac{e(P_1, Q_1)}{e(P_2, Q_2)} = e(P_1, Q_1)e(P_2, -Q_2)$, and if we take P_1 and P_2 with the same order, we can so utilize the same algorithm of Miller to calculate the inverse of two pairing. The only things we change is instead of $f_1 \leftarrow f_1^2 \times \frac{l_1(Q_1)}{v_1(Q_1)}$ we calculate $f_1 \leftarrow f_1^2 \times \frac{l_1(Q_1)}{v_1(Q_1)} \times \frac{l_1(Q_2)}{v_1(Q_2)}$ also instead of

$$f_1 \leftarrow f_1 \times \frac{l_2(Q_1)}{v_2(Q_1)} \text{ we calculate } f_1 \leftarrow f_1 \times \frac{l_2(Q_1)}{v_2(Q_1)} \times \frac{l_2(Q_2)}{v_2(Q_2)}.$$

The calculation of the pairing is ineffective until the invention of the algorithm of Miller in 1986.

Miller(P, Q, r)
<p>Input : $\mathbf{r} = (r_n \dots r_0)$ (binary representation), $P \in E[r](\subset E(F_q))$ and $Q \in G_1(\subset E(F_{q^k}))$</p> <p>Output : $f_{r,P}(Q) \in G_3(\subset F_{q^k}^*)$</p> <p>$T \leftarrow P$ $f_1 \leftarrow 1$ for $i = n - 1$ to 0 do 1 : $T \leftarrow [2]T$ $f_1 \leftarrow f_1^2 \times \frac{l_1(Q)}{v_1(Q)}$ l_1 is the tangent to the curve in T. V_1 is the vertical to the curve in $[2]T$. 2 : if $r_i=1$ then $f_1 \leftarrow f_1 \times \frac{l_2(Q)}{v_2(Q)}$ l_2 is the line passing through the point TP V_2 is the vertical to the point $P + T$. Output : Return f_1</p>

2.1.8 Haching on an elliptic Curve

In the cryptosystem of Boneh and Franklin there is, the problem of Hashing Function in an elliptic curve selected. And to do it we remember the method suited by Boneh Franklin

Map to point

0. Project the ID using : $H_1 : \text{ID} \in \{0,1\}^* \longrightarrow y_0 \in F_p$
1. Calculate $x_0 = (y_0^2 - 1)^{\frac{1}{3}} = (y_0^2 - 1)^{\frac{2p-1}{3}} \in F_p$.
2. Let $Q = (x_0, y_0) \in E(F_p)$ after calculate $Q_{ID} = lQ \in G$.
3. Output $\text{MapToPoint}(y_0) = Q_{ID}$.

2.1.9 Cryptosystems in Competition

The cryptosystems in competition are Boneh and Franklin, Skai Kasarah, Boneh Boyen, Water, Gentry. In this article we choose them, taking into account the most recent changes to make them effective. So for Boneh and Franklin we prefer to use that of Galnido [25] instead of the version of Boneh and Franklin. Because Galnido provide reduction in the advantage of Boneh Franklin. More, this latter is valid only on supersingular curve, as it uses symmetric pairing. By contrast, Galnido use asymmetric pairing of type II and he established his argument based on them. Following [26] the asymmetric pairing, with which we can use ordinary curves are more convenient in implementations than the symmetric one.

Boneh-Franklin (Galindo-Full Version)
<p>Setup. Let (G_1, G_2, G_T, ψ) a bilinear group. Choose a generator $P_2 \in G_2$ and set $P_1 = \psi(P_2)$. Next pick $s \leftarrow Z_p$ and set $Q_{pub} = sP_2 \in G_2^* \rightarrow P_{pub} = sP_1 \in G_1^*$. Choose cryptographic hash functions $H_1 : \{0, 1\}^* \leftarrow G_2^*$, $H_2 : G_T \leftarrow \{0, 1\}^n$, $H_3 : \{0, 1\}^n \times \{0, 1\}^n \leftarrow Z_p^*$, $H_4 : \{0, 1\}^n \leftarrow \{0, 1\}^n$. The message space is $M = \{0, 1\}^n$ and the ciphertext space is $C = G_1^* \times \{0, 1\}^n \times \{0, 1\}^n$.</p> <p>Extract. For a given string $ID \in \{0, 1\}^*$, compute $Q_{ID} = H_1(ID)$ and set the private key d_{ID} to be $d_{ID} = sQ_{ID} \in G_2^*$.</p> <p>Encrypt. To encrypt $M \in \{0, 1\}^n$ under identity ID, compute $Q_{ID} = H_1(ID) \in G_2^*$, choose $\sigma \leftarrow \{0, 1\}^n$, set $r = H_3(\sigma, M) \in Z_p^*$ and finally $C = \langle rP_1, \sigma \oplus H_2(g_{ID}^r), M \oplus H_4(\sigma) \rangle$ where $g_{ID} = e(P_{pub}, Q_{ID}) \in G_T$.</p> <p>Decrypt. Let $C = \langle U, V, W \rangle \in C$ be a ciphertext under the identity ID. To decrypt C using the private key $d_{ID} \in G_2^*$ do :</p> <ol style="list-style-type: none"> 1. Compute $V \oplus H_2(e(U, d_{ID})) = \sigma$. 2. Compute $W \oplus H_4(\sigma) = M$. 3. Set $r = H_3(\sigma, M)$. Check that $U = rP$. If not, reject the ciphertext. 4. Output M.

Sakai-Kasaharah (ChenCheng-Full Version)
<p>Setup. Let (G_1, G_2, G_T, ψ) a bilinear group. Choose a generator $P_2 \in G_2$ and set $P_1 = \psi(P_2)$. Next pick $s \leftarrow Z_p$ and set $Q_{pub} = sP_2 \in G_2^* \rightarrow P_{pub} = sP_1 \in G_1^*$. Choose cryptographic hash functions $H_1 : \{0, 1\}^* \leftarrow G_2^*$, $H_2 : G_T \leftarrow \{0, 1\}^n$, $H_3 : \{0, 1\}^n \times \{0, 1\}^n \leftarrow Z_p^*$, $H_4 : \{0, 1\}^n \leftarrow \{0, 1\}^n$. The message space is $M = \{0, 1\}^n$ and the ciphertext space is $C = G_1^* \times \{0, 1\}^n \times \{0, 1\}^n$.</p> <p>Extract : Given an identifier string $ID_A \in \{0, 1\}^n$ of entity A, M_{pk} and M_{sk}, the algorithm returns $d_A = \frac{1}{s + H_1(ID_A)} P_2$</p> <p>Encrypt : Given a plaintext $m \in M$, ID_A and M_{pk}, the following step are formed :</p> <ol style="list-style-type: none"> 1. pick a random $\sigma \in \{0, 1\}^n$ and compute $r = H_3(\sigma, m)$ 2. Compute $Q_A = H_1(ID_A)P_1 + P_{pub}$, $g^r = e(P_1, P_2)^r$ Set the ciphertext to be $C = (rQ_A, \sigma \oplus H_2(g^r), m \oplus H_4(\sigma))$ <p>Decrypt : Given a ciphertext $C = (U, V, W) \in C$, ID_A, d_A and M_{pk}, follow the steps</p> <ol style="list-style-type: none"> 1. Compute $g' = e(U, d_A)$ and $\sigma' = V \oplus H_2(g')$ 2. Compute $m' = W \oplus H_4(\sigma')$ and $r' = H_3(\sigma', m')$ 3. If $U \neq r'(H_1(ID_A)P_1 + P_{pub})$ output \perp else return the m' as the plaintext

Boneh-Boyen
BB1(Full Version)
<p>Setup : To generate IBE system parameters, pick $\omega, \alpha, \beta, \gamma \in Z_p$, and output, params = $\{ P, P_1 = \alpha P, P_2 = \beta P, v_0 = e(P, \hat{P})^\omega \} \in G_1^3 \times G_t$, masterk = $(\hat{P}, \omega, \alpha, \beta) \in G_2 \times Z_p^4$.</p> <p>Let g_1 and g_2 be the respective generators of some bilinear group pair (G_1, G_2) of prime order p, And let $e : G_1 \times G_2 \rightarrow G_t$ be a bilinear pairing map.</p> <p>The availability of three cryptographic hash functions viewed as random oracles graphic hash functions $H_1 : \{0, 1\}^* \leftarrow Z_p, H_2 : G_t \leftarrow \{0, 1\}^n, H_3 : G_t \times \{0, 1\}^n \times G_1 \times G_2 \leftarrow Z_p$.</p> <p>The message space is $M = \{0, 1\}^n$ and The ciphertext space is $C = G_1^* \times \{0, 1\}^n \times \{0, 1\}^n$.</p> <p>Extract : To extract from masterk a private key d_{ID} for an identity $ID \in \{0, 1\}^l$, pick a random $r \in Z_p$ and output $d_{ID} = (d_0 = (\omega + (\alpha H_1(ID) + \beta)r)\hat{P}, d_1 = r\hat{P})$.</p> <p>Encrypt : Given a plaintext $m \in M, ID_A$ and M_{pk}, the following step are formed :</p> $C = \begin{cases} c = M \oplus H_2(k = v_0^s), \\ c_0 = sP, \\ c_1 = H_1(ID)sP_1 + sP_2, \\ t = s + H_3(k, c, c_0, c_1) \bmod p \end{cases}$ <p>where $M \in \{0, 1\}$ is the message, $ID \in \{0, 1\}$ is the recipient identifier, and $s \in Z_p$ is a random ephemeral integer.</p> <p>Decrypt : Given a ciphertext C and a private key $d_{ID} = (d_0, d_1)$, compute, $k = \frac{e(c_0, d_0)}{e(c_1, d_1)}, s = t - H_3(k, c, c_0, c_1)$. If $(k, c_0) \neq (v_0^s, sP)$, output \perp; otherwise, output, $M = c \oplus H_2(k)$.</p>
BB2 (Version CPA)
<p>Setup outputs $\text{Msk} \leftarrow (a, b)$ and $\text{Pub} \leftarrow (P, P_a = aP, P_b = bP, v = e(P, \hat{P}))$ for $a, b \in F_p$ chosen at random.</p> <p>Extract(Msk, Id) outputs $Pvk_{Id} \leftarrow (r_{Id} = r, \hat{d}_{Id} = \frac{-1}{a + Id + br}\hat{P})$ for $r \in F_p$</p> <p>Encrypt(Pub, Id, Msg, s) outputs $\text{Ctx} \leftarrow (c_0 = \text{Msg}.v^s, c_1 = sP_a + sIdP, c_2 = sP_b)$.</p> <p>Decrypt(Pub, Pvk_{Id}, Ctx) outputs $\text{Msg}' \leftarrow c_0.e(c_1 + r_{Id}c_2, \hat{d}_{Id}) \in G_t$.</p>

Water (Naccache-Version CPA)

Setup : Choose a secret parameters $\alpha \in Z_p$ at random, choose a random generator $g \in G$ and set the value $g_1 = \alpha g$ also choose at randomly $g_2 \in G$. The authority choose a random value $u' \in G$ and a random n length vector $U=(u_i)$ chosen at random from G . The publish parameters are $\text{params} < g, g_1, g_2, u', U >$ the master secret is αg_2

Key Generation : Let $v = (v_1, \dots, v_n) \in (\{0, 1\}^a)^n$ be an identity, Let r be random in Z_p . The private key d_v for identity v is constructed as : $d_v = (\alpha g_2 + r(u' + \sum_{i=1}^n u_i), rg)$

Encryption : A message $M \in G_1$ is encrypted for an identity v as follows. A value $t \in Z_p$ is chosen at random. The ciphertext is then constructed as : $C = (e(g_1, g_2)^t M, t.g, t.(u' + \sum_{i=1}^n u_i))$

Decryption : Let $C = (c_1, c_2, c_3)$ be a valid encryption of M under the identity v . Then C can be decrypted by $d_v = (d_1, d_2)$ as : $c_1 \frac{e(d_2, C_3)}{e(d_1, C_2)} = M$

Gentry(Full-Version)

Setup : The PKG picks a random generators $< g, h_1, h_2, h_3 >$ and a random $\alpha \in Z_p$. It sets $g_1 = \alpha g \in G$. It chooses a hash function H from a family of universal one-way hash functions. The public params and private master-key are given by $\text{params} = < g, g_1, h_1, h_2, h_3, H >$ master-key = α

Key Gen : To generate a private key for identity $ID \in Z_p$, the PKG generates random $r_{ID,i} \in Z_p$ for $i \in \{1, 2, 3\}$ and output the private key $d_{ID} = \{(r_{ID,i}, h_{ID,i}) : i \in \{1, 2, 3\}, \text{ where } h_{ID,i} = \frac{1}{\alpha - ID}(h_i + (r_{ID,i}g))\}$. If $ID = \alpha$, the PKG aborts.

Encrypt : To encrypt $m \in G_T$ using identity $ID \in Z_p$, the sender generates random $s \in Z_p$ and send the ciphertext $C = \begin{cases} u = sg_1 + (-sID)g, \\ v = e(g, g)^s, \\ w = m.e(g, h_1)^{-s}, \\ y = e(g, h_2)^s e(g, h_3)^{s\beta} \end{cases}$

Above, for $C = (u, v, w, y)$ we set $\beta = H(u, v, w)$

Decrypt : To decrypt ciphertext $C = (u, v, w, y)$ with ID the recipient sets $\beta = H(u, v, w)$ and test whether $y = e(u, h_{ID,2}) h_{ID,3}^\beta v^{r_{ID,2} + r_{ID,3}\beta}$. If the check fails, the recipient output \perp . Otherwise, it outputs $m = w.e(u, h_{ID,1}) v^{r_{ID,1}}$

Justification of the Choose

We are making our choose based on the recent modifications concerning the cryptosystems in competition. For that of Boneh and Franklin, we have justified the version of Galnido. As that of

Skai Kasarah, we prefer to use the version of Chen-Cheng [19] which is CCA secure. As far as concerned, the version of BB1 we will utilize the Random oracle version, such that BB1 has a lot of versions : Random Oracle, selectiveID, and also Standard Model. We will only play on the H_1 , but we prefer the first one, because we have the cryptosystem of Water which has the same syntax as BB1 and is under Standard Model. As long as, that of Water we will use the version of Nackache which utilize the Words instead of the alphabet. And this reduce the complexity

2.2 Efficient Comparison

As we have signaled Xavier. Boyen in 2008 essayed to make the comparison [11] between Boneh Franklin, Skai Kasarah and BB1. By counting for example the numbers of the parameters for each cryptosystem, the groups associates, the propriety associates. More he has calling to the standardization of the cryptosystem BB1 [10] using the same method. Unfortunately his essay isn't practical for the reason that he don't compute the complexity exact (spatial and temporal) for each cryptosystem. He fixed only the basis and he begun to compute following the number of the parameters. He posed some critters and he verified if only the cryptosystems has it or not without demonstrate any classification. By contrast, in our comparison we will follow another strategy. We pose a scale which we make in the consideration the utility of the propriety, this allow us to precise the best cryptosystem.

2.2.1 Comparison in the level Security

Before staring the comparison in the level of security we remember firstly the following things :

BF	SK	BB1	BB2	Water	Gentry
RO	RO	RO & sID	RO & sID	SM	SM
BDHP	BDHIP	BDHP	DBDHIP	DBDHP	Dq-ABDHP
CCA	CCA	CPA	CPA	CPA	CCA
SiE-BDHP	BCAA1	PDL	BCAA1	PDL	BCAA1

To rank the crypto systems in direction security, we give the scale following the usefulness of each propriety. Concerning the model utilized : RO is the worst case as long as SM is the better, until sID is between them, therefore : RO (rank 3), sID (rank 2), SM (rank 1). But because of the very great dangers of RO [22] and as we presented a few of them in section 2.1.2 we double these coefficients in the table below. In the other part, because of the utility of the anonymity for the security, as it can early block the activity of the opponent we reducing the rank to 0 for those that have it and we give 2 to those they don't have it. For the remaining criteria we follow the classification we done in the section 2.1.1 ; 2.1.4

TABLE 1 – classification in the level security

	BF	SK	BB1	BB2	Water	Gentry
Model	6	6	4	4	2	2
Pro_{DH}	1	2	1	4	3	4
Avd	2	3	5	6	1	4
Simu	0	0	1	1	1	0
$Pro_{DH_{priv}}$	2	3	1	3	1	3
Ano	0	2	2	2	2	0
Sum	11	16	14	20	10	13
Class	(2 ^{sd})	(5 th)	(4 th)	(6 th)	(1 st)	(3 th)

2.2.2 Comparison in the level Complexity

In [10][11] Xavier Boyen tried to establish a base, from which he tried to compute the time for the crypto systems that are affected. But we can say that his results are not accurate enough, because, he doesn't take into account some operations such as : inverse, multiplication etc. By contrast in our study we compute the most possible operations. More our complexity can combine between spatial and temporal

Complexity associate

We assemble our own complexity in the following tables.

With the fact that in table III we set the parameters, with a manner to reduce more possibly the calculation, for example, instead of placing $g = e(P_1, P_2)$ (in SK cryptosystem) in the Encrypt at which we will recalculate it each time, we publish it among the Params

In the table IV the following symbol significate :

C : Complexity ; Mul_{sca} : Multiplication Scalar ; Exp_{ffi} : Exponentiation in the finite field ; Inv_{ffi} : Inversion in the finite field ; Mul_{ffi} : Multiplication in the finite field ; pair : Pairing ; Inv of 2 pair : Inversion of two pairing

TABLE 2 – Parameter Associate

BF_{Ga}	SK_{CC}	
sP_1	$sP_1 ; g = e(P_1, P_2)$	
Q_{ID} (map to point) ; sQ_{ID}	$\frac{1}{s+H_1(ID)}P_2$	
$u=rP_2 ; e(P_{pub}, Q_{ID})^r$	$Q = H_1(ID)P_1 + P_{pub}; g^r; u = rQ$	
$e(u, d_{ID})$	$e(u, d_{ID}) ; r'Q_A$	
BB1	BB2	$Water_{Na}$
$\alpha P_1 ; \beta P_2 ; e(P, \hat{P}) ; v_0$	$aP_1 ; bP_2 ; e(P, \hat{P})$	$\alpha g_1 ; v = e(g_1, g_2)$
$(\omega + r(\alpha H_1(ID) + \beta))\hat{P} ; r\hat{P}$	$\frac{1}{a+ID+br}\hat{P}$	$\alpha g_2 + r(U' + \sum_{i=1}^n U_i) ; rg$
$v_0^s ; sP ; H_1(ID)sP_1 ; sP_2$	$m.v^s ; sP_a ; sIdP ; sP_b$	$v^t ; tg ; t(U' + \sum_{i=1}^n U_i)$
$\frac{e(c_0, d_0)}{e(c_1, d_1)} ; v_0^s ; sP$	$c_0.e(c_1 + rIdc_2, \hat{d}_{Id})$	$c_1.\frac{e(c_3, d_2)}{e(c_2, d_1)}$

Gentry
$v_0 = e(g, g); v_1 = e(g, h_1); v_2 = e(g, h_2); v_3 = e(g, h_3)$
$\frac{1}{\alpha-ID}(h_i + r_{ID,i}g), i \in \{1, 2, 3\}$
$u; v_0^s; m.v_1^{-s}; v_2^s.v_3^{s\beta}$
$y = e(u, h_{ID,2} + \beta h_{ID,3})v_0^{r_{ID,2}+r_{ID,3}\beta}; w.e(u, h_{ID,1})v^{r_{ID,1}}$

TABLE 3 – Complexity associate

BF_{Ga}	SK_{CC}
$C(Mul_{sca})$	$C(Mul_{sca})+C(\text{pair})$
$C(\text{map to point})+C(Mul_{sca})$	$C(Inv_{ffi})+C(Mul_{sca})$
$C(Mul_{sca})+C(\text{pair})+C(Exp_{ffi})$	$2C(Mul_{sca})+C(Exp_{ffi})$
$C(\text{pair})$	$C(\text{pair})+C(Mul_{sca})$
BB1	BB2
$2C(Mul_{sca})+C(\text{pair})+C(Exp_{ffi})$	$2C(Mul_{sca})+C(\text{pair})$
$2C(Mul_{ffi})+2C(Mul_{sca})$	$C(Inv_{ffi})+C(Mul_{sca})+C(Mul_{ffi})$
$3C(Mul_{sca})+C(Exp_{ffi})+C(Mul_{ffi})$	$3C(Mul_{sca})+C(Exp_{ffi})+2C(Mul_{ffi})$
$C(\text{Inv of 2 pair})+C(Exp_{ffi})+C(Mul_{sca})$	$C(Mul_{ffi})+C(\text{pair})+C(Mul_{sca})$
$Water_{Na}$	Gentry
$C(Mul_{sca})+C(\text{pair})$	$4C(\text{pair})$
$4C(Mul_{sca})$	$3C(Mul_{sca})+C(Inv_{ffi})$
$3C(Mul_{sca})+C(Exp_{ffi})+C(Mul_{ffi})$	$2C(Mul_{sca})+4C(Exp_{ffi})+C(Inv_{ffi})+2C(Mul_{ffi})$
$C(Mul_{ffi})+C(\text{Inv of 2 pair})$	$4C(Mul_{ffi})+2C(\text{pair})+C(Mul_{sca})+2C(Exp_{ffi})$

Observation : To calculate the Multiplication Scalar we consider in this article that the operation of adding and doubling are equal so for

example : $(U' + \sum_{i=1}^n U_i)$ is considered as one Scalar Multiplication.

Complexity Neighboring

In this section we begin to fix the complexity for each cryptosystem. We can say that they are a complexity neighbor, since we do not take into account : addition, subtraction, calculation of hashed functions... More we balance between the complexity of square with that of multiplication. Our method help us to have a nearest comparison between the cryptosystem's in competition, because we will concentrate only on the main arithmetic (operation used) : multiplication, square, exponentiation, scalar multiplication in each cryptosystem.

Following [27] we have :

1. $C(\text{compute of } m \times n) = O((\log n)^2)$
2. $C(\text{compute of } \gcd(m, n)) = C(\text{compute of } m^{-1}) = O((\log n)^3) = C(\text{compute of } m^{-1} \pmod{n}) =$

$O((\log n)^3)$

For the exponentiation we consider in this article the algorithm Right-to-left binary exp [28] which has complexity equivalent to :

$(\frac{1}{2}\lg n)\text{Mu} + (\lg n)\text{Sq} = (\frac{3}{2}\lg n)\text{Mu}$ (as declared $C(\text{Mu})=C(\text{Sq})$). Those complexity are not a persuade complexity and to make an exact one we will use the newest method used in the literature. But this help us to order the main operation in arithmetic, as [29] we have according to those complexity : $C(\text{multiplication}) < C(\text{inverse}) < C(\text{exponentiation})$

In [11] Boyen balance between exponentiation x^n and the scalar multiplication $[n]P$ as we can apply the same operations to crush the n . This is not true, because we must consider for $[n]P$ an additional complexity :

Following [29], in jacobian coordinate we have :

$C(\text{ECADD})=12\text{Mu}+2\text{Sq}=14O((\log n)^2)$ ($C(\text{Mu})=C(\text{Sq})$ the $Z \neq 1$)

And $C(\text{ECDBL})=7\text{Mu}+5\text{Sq}=13O((\log n)^2)$ ($a \neq -3$)

With ECADD : designs elliptic curve point adding $P+Q$, ECDBL : designs elliptic curve point doubling $2P$.

Also following [29] and using NAF algorithm we have :

$C(dP)=(n-1)\text{ECDBL}+\frac{(n-1)}{3}\text{ECADD}=13(n-1)O((\log n)^2)+14\frac{(n-1)}{3}O((\log n)^2)=\frac{53}{3}(n-1)O((\log n)^2)$.

And $C(2^n P)=4n\text{Mu}+(4n+2)\text{Sq}=(8n+2)O((\log n)^2)$ i.e for $d=2^n$.

According to algorithm Maptopoint we have :

$C(\text{Maptopoint})= C(1 \text{ square}) + C(1 \text{ cubic root}) + C(1 \text{ multiplication scalar})$

So : $C(\text{Maptopoint}) = O((\log n)^2) + O(\lg \lg n) + \frac{53}{3}(n-1)O((\log n)^2)$ (complexity of the cubic root is $O(\lg \lg n)$ following an algorithm in [28])

For the complexity of the pairing we will take into consideration, as possible all the reduction we can apply to reduce the pairing. We take for example Tate because Weil is heavy (two time bigger than Tate). So we have :

$C(\text{pairing}=\text{Tate})=C(\text{Miler})+C(\text{Exponentiation})$, since $t_r = (f_r)^{\frac{q^k-1}{r}}$

With a naive calculate we have :

Starting with the complexity of the algorithm of Miller. We neglect as customary to accelerate the compute, the second tranche of the algorithm of Miller supposing that our r (for example $r=3^{97} + 3^{49} + 1$, so we can neglect 3 bit in front of 94 bit) is cruse.

Firstly, we have $t_r = (f_r(D_Q))^{\frac{q^k-1}{r}} = (\frac{f_{r,P}(Q+S)}{f_{r,P}(S)})^{\frac{q^k-1}{r}}$ with $D_Q = [Q+S]-[S]$ for an arbitrary chosen S in the elliptic curve concerned. The algorithm of Miller is resumed in table 4

In this algorithm, we need three stages : (1) computation of ECDBL (we neglect ECADD) (2) computation of $l_1(Q+S), l_1(S), v_1(Q+S), v_1(S)$ (3) update of f_1

According to [29] we have so : $C(\text{Miller}) = r \log 2(4Mu_k + 2Sq_k + (6k+7)Mu + 7Sq)$ with $r \log 2$ is the number of iterations. If r is in the same level of security as n , we will have :

$C(\text{Miller}) = n \log 2(4Mu_k + 2Sq_k + (6k+7)Mu + 7Sq)$.

NB :

1. Even if we are basing in a work[29] made in 2003, but this complexity is nearest to the one[30] done in 2009 section II.2.1. And in this latter the author don't take into account $l_1(Q+S)$, $v_1(Q+S)$, multiplication : $l_1(Q+S) \times v_1(S)$, $l_1(S) \times v_1(Q+S)$
2. k designs the embedding degree of the field used. For example F_{p^k} ; Mu_k : multiplication in this field; Sq_k : squaring in this field.
3. Certain work use twist which eliminate the calculate of v_1 , this is possible for embedding degree

TABLE 4 – first tranche

Compute of $\frac{f_{r,P}(Q+S)}{f_{r,P}(S)}$: first tranche
Input : $r = (r_n \dots r_0)$ (binary representation), $P \in E[r](\subset E(F_q))$ and $Q \in G_1(\subset E(F_{q^k}))$ $S \in G_1(\subset E(F_{q^k}))$ Output : $f_{r,P}(Q) \in G_3(\subset F_{q^k}^*)$ $T \leftarrow P$ $f_1 \leftarrow 1$ for $i = n - 1$ to 0 do 1 : $T \leftarrow [2]T$ $f_1 \leftarrow f_1^2 \times \frac{l_1(Q+S)}{l_1(S)} \times \frac{v_1(S)}{v_1(Q+S)}$ l_1 is the tangent to the curve in T . v_1 is the vertical to the curve in $[2]T$.

divided by 2, 3, 4, 6. But we don't take it into consideration in this work

4. According to [31], for $k=2^i 3^j$ $Mu_k = 3^i 5^j Mu$; $Mu_k \sim Sq_k$ so $Sq_k \cong 3^i 5^j Mu$.

We take $k=2^i 3^j$ as an experiment embedding to make our comparison, this because of last step : step number 4. And the fact that $C(Mu) \simeq C(Sq)$. So :

$$C(\text{Miller}) = n \log 2 ((6.3^i 5^j + (6k + 14)) O((\log n)^2)).$$

For $k=12$ and in a level of security $=80$. We have : $C(\text{Miller}) = 28480 \log 2 O(6400(\log 2)^2)$.

$$C(\text{pairing}) = n \log 2 ((6.3^i 5^j + (6k + 14)) O((\log n)^2)) + (\frac{3}{2} \lg n) O((\log n)^2)$$

We move now to the inversion of two pairing :

According to section 2.1.7 instead of calculate $\frac{t_{r_1}(D_{r_1}(D_{Q_1}))}{t_{r_2}(D_{r_2}(D_{Q_2}))} = \frac{(f_{r_1, P_1}(D_{Q_1}))^{\frac{q^k-1}{r_1}}}{(f_{r_2, P_2}(D_{Q_2}))^{\frac{q^k-1}{r_1}}}$, if P_1 and P_2 have the

same order $r=r_1=r_2$, we calculate only $t_r(D_r(D_{Q_1})) \times t_r(D_r(D_{Q_2}))$. This reduce the complexity from $4Mu_k$ to only $2Mu_k$ (as inversion in F_{p^k} is approximated to $4Mu_k$ following [29])

Using this, the technique proposed in the section 2.1.7 and complexity given in [29] (first tranche), we have :

$$C(\text{Inversion of Tate Pairing}) = n \log 2 (2(4Mu + 6Sq) + 2(3Mu + 1Sq) + 4(3kMu) + 4Mu_k + 2Sq_k) + 1C(\text{exponent}) = (28+12k + 6.3^i 5^j)Mu + \frac{3}{2} \log n O(\log n^2) = n \log 2 (28+12k+6.3^i 5^j) O((\log n)^2) + \frac{3}{2} \log n O(\log n^2)$$

We will use all this complexity in the following section when we have ambiguity.

Efficient Classification

To classify our cryptosystems we compared them following each taps : Params, Extract, Encrypt, Decrypt. So we have following the complexity in table 3 and the complexity declared in the previous section :

It is clear from table 3 that : $(BF - Gentry)_{Params} < (SK - ChenCheng)_{Params} \& Water_{Params} < BB2_{Params}$. To compare $BB1_{Params}$ and $Gentry_{Params}$ we will compare only $2C(Mul_{sca}) + C(Exp_{ffi})$ and $3C(\text{pair})$. As we have $\frac{106}{3}(n-1) + \frac{3}{2} \log n < (\log 2^n)(18.3^i . 5^j + 3(6k+14) + \frac{9}{2} \log n)$, $BB1_{Params} < Gentry_{Params}$.

So : $(BF - Gentry)_{Params} < (SK - ChenCheng)_{Params} \& Water_{Params} < BB2_{Params} < BB1_{Params} < Gentry_{Params}$.

For the Extract, the fact that Mul_{sca} has in its formulate an Mul and Sq multiplied by n, will help us in a more statement. The only ambiguity that we can have is between BF and BB1, but as we

have $C(\text{square root}) < C(\text{Mul})$ we will have :

$$(SK - \text{ChenCheng})_{\text{Extract}} < BB2_{\text{Extract}} < (BF - \text{Galnido})_{\text{Extract}} < BB1_{\text{Extract}} < \text{Gentry}_{\text{Extract}} < \text{Water}_{\text{Extract}}.$$

In the level Encrypt we have regrouped the complexity for each cryptosystem, using the fact that an inversion in F_{p^k} is approximated to $4Mu_k$ [29] (for Gentry) we find that :

$$(SK - \text{ChenCheng})_{\text{Encrypt}} < BB1_{\text{Encrypt}} \& \text{Water}_{\text{Encrypt}} < BB2_{\text{Encrypt}} < \text{Gentry}_{\text{Encrypt}} < (BF - \text{Galnido})_{\text{Encrypt}}$$

As far as for the Decrypt we have :

$$(BF - \text{Galnido})_{\text{Decrypt}} < (SK - \text{ChenCheng})_{\text{Decrypt}} < \text{Water}_{\text{Decrypt}} < BB2_{\text{Decrypt}} < BB1_{\text{Decrypt}} < \text{Gentry}_{\text{Decrypt}}.$$

The classification between $(BF - \text{Galnido})_{\text{Decrypt}} - (SK - \text{ChenCheng})_{\text{Decrypt}}$; as well as $BB2_{\text{Decrypt}} - BB1_{\text{Decrypt}}$ and $BB1_{\text{Decrypt}} - \text{Gentry}_{\text{Decrypt}}$ are clair. We have an ambiguity between $\text{Water}_{\text{Decrypt}}$ and $BB2_{\text{Decrypt}}$, $\text{Water}_{\text{Decrypt}}$ and $(SK - \text{ChenCheng})_{\text{Decrypt}}$. But as we have $n \log 2(28 + 12k + 6 \cdot 3^i \cdot 5^j) + 1 > n \log 2(6 \cdot 3^i \cdot 5^j + 6k + 14) + \frac{53}{2}(n-1)$, because $(14 + 6k) \log 2 + 1 > \frac{53}{2}(n-1)$ (we can take the minimal case $k=2$) we can so conclude.

TABLE 5 – Classification

	BF_{Gal}	SK_{Ch-Chg}	BB1	BB2	Water	Gentry
Params	1	2	4	3	2	5
Extract	3	1	4	2	6	5
Encrypt	5	1	2	3	2	4
Decrypt	1	2	5	4	3	6
Sum	10	6	15	12	13	20
Class	(2 ^{sd})	(1 st)	(5 th)	(3 th)	(4 th)	(6 th)

2.3 Final Classification

As a consequent of all what we have seen before, we regrouped our results in the following table :

	BF	SK	BB1	BB2	Water	Gentry
Class TABLE 1	(2 ^{sd})	(5 th)	(4 th)	(6 th)	(1 st)	(3 th)
Class TABLE 5	(2 ^{sd})	(1 st)	(5 th)	(3 th)	(4 th)	(6 th)
Sum	4	6	9	9	5	9
Final $Class_1$	(1 st)	(3 th)	(4 th)	(4 th)	(2 ^{sd})	(4 th)

2.4 Propriety Associate

In this section as [11] we also enriched our study with the additional properties such as : Multi-recipient encryption, Threshold secret sharing, Hierarchical identities. Our comparison is totally difference from that of [11]. Because we do not mark only the property as [11] to the crypto systems, but we test the best crypto system which verify the property wished.

We make firstly the following recall with a little details :

Multi-recipient encryption (1) : Is the act of encrypting a single message to multiples users. So this priority requires a **small Encrypt**

Threshold secret sharing (2) : Is the fact of dividing the key Master on several authorities, to avoid the concentration on one. And each of them has the advantage to calculate a corresponding

private key. So this priority requires a **small Extract**

Hierarchical Identity (3) : Is the fact of arranging multiples identities in the hierarchy (many authorities classify in an hierarchy) using the same Params. So each of the super authority generate the corresponding key to its down. This priority requires **Extract and Encrypt smaller**. Its ranking is calculated as (Extract + Encrypt)

	BF	SK	BB1	BB2	Water	Gentry
M-r enc (1)	5	1	2	3	2	4
Th s sh (2)	3	1	4	2	6	5
Hi id (3)	4	1	3	2	4	5
Sum	12	3	9	7	12	14
$Class_2$	(4 th)	(1 st)	(3 ^{sd})	(2 th)	(4 th)	(5 th)
Specific $Class_{Fi} = Class_1 + Class_2$	(2 st)	(1 st)	(4 ^{sd})	(3 th)	(3 st)	(5 th)

3 Second goal

In the following sections, we will give an efficient schemes IBE/HIBE in the model selective ID. A comparison in terms of performance and complexity with BB1 and BBG scheme is in favor of our scheme.

3.1 Preliminaries

To be familiarized with the difference between IBE and HIBE, we give in the following the functionality of each others.

3.1.1 Functionality of IBE :

An IBE system contains four basic components in its construction :

Setup : A trusted central authority manages the parameters with which keys are created. This authority is called the Private Key Generator or PKG. The PKG takes a security parameter k and returns **params** (system parameters) and **master-key**. The system parameters will be publicly known, while the master-key will be known only to the (PKG).

Extract : Takes as input **params**, **master-key**, and an arbitrary ID_R , it returns a private key d_{ID_R} .

Encryption : When Alice wishes to encrypt a message to Bob, he encrypts the message to him by computing or obtaining the public key, and then encrypting a plaintext message M with params, ID_{Bob} to obtain ciphertext C .

Decryption : When Bob has C , he contact the PKG to obtain the private key S_{Bob} , he decrypts C to obtain the plaintext message M .

3.1.2 IBE security notions

As it was known Boneh and Franklin define in [2] a chosen ciphertext security for IBE systems under a chosen identity attack. In this model the adversary is allowed to adaptively chose the public key it wishes to attack. In [13] Canetti, Halevi, and Katz define another notion it is a weaker notion of security. In this model the adversary commits ahead of time to the public key it will attack.

Before giving its functionality we recall firstly that the security of a cryptographic scheme combining the possible goals and attack models. The most important goal are : indistinguishability (IND/sIND), Semantic Security. Regarding attacks we have : chosen-plaintext attacks (CPA), chosen-ciphertext attacks (CCA). The relation between all this was given in [32].

Definition :IND-ID/sID-{CCA, CPA}

Let $\Gamma = (S, X, E, D)$ be an IBE scheme, and let $A = (A_0, A_1, A_2)$ be any 3-tuple of PPT oracle algorithms. For $ATK = ID/sID\text{-}CPA, ID/sID\text{-}CCA$, we say Γ is IND/sID-ATK secure if for any 3-tuple of PPT oracle algorithms $A, | \wp r(1) - \wp r(2) | \in neg$, where

$$\wp r(i) = \left\{ \begin{array}{l} v = 0 \\ \left(\begin{array}{l} (id, \gamma) \leftarrow A_0(1^l) \\ (pms, mk) \leftarrow S(1^l); \\ ((m^{(1)}, m^{(2)}, id_{ch}), \sigma) \leftarrow A_1^{O_1, O_2}(pms, id, \gamma) \\ c \leftarrow E(pms, id_{ch}, m^{(i)}); \\ v \leftarrow A_2^{O_1, O_2}(\sigma, (id_{ch}, c)) \end{array} \right) \end{array} \right\}.$$

The expression represent the oracles O_1, O_2 . Additionally, $m^{(1)}$ and $m^{(2)}$ are required to have the same length ; neither A_1 nor A_2 are allowed to query O_1 on the challenge identity id_{ch} , and A_2 can not query O_2 on the challenge pair (id_{ch}, c) . These queries may be asked adaptively (like CCA2 after phase 2), that is, each query may depend on the answers obtained to the previous queries.

3.1.3 Functionality of HIBE

Like IBE system, the Hierarchical Identity Based Encryption (HIBE) system consists of four algorithms [15][16] : **Setup, KeyGen, Encrypt, Decrypt**.

In HIBE, however, identities are vectors, a vector of dimension k represents an identity at depth k . The Setup algorithm generates system parameters, denoted by $params$, and a master key $master\text{-}key$. We refer to the master-key as the private key at depth 0 and note that an IBE system is a HIBE where all identities are at depth 1. Algorithm KeyGen takes as input an identity $ID = (I_1, \dots, I_k)$ at depth k and the private key $d_{ID|k-1}$ of the parent identity $ID|k-1 = (I_1, \dots, I_{k-1})$ at depth $k-1$, and then outputs the private key d_{ID} for identity ID . The encryption algorithm encrypts messages for an identity using $params$ and the decryption algorithm decrypts ciphertexts using the private key.

3.1.4 The main approach of IBE

We can classify the cryptosystems of IBE in three categories :

- Full-Domain-Hash approach : In this model we project in the elliptic curve instead of the finite field, its prototype is summarized by the idea of Boneh-Franklin [2].
- Exponent-Inversion approach : In this approach the identity key to be used in the Extract is as an inverse. The second scheme of Boneh-Boyen (BB2)[4], that's of Sakai-Kasahara (SK) [3], also Gentry [6] work with this approach.
- Commutative-Blinding approach, defined by the first IBE scheme of Boneh-Boyen (BB1)[4]. It is based on the idea of creating, from two or more secret coefficients, two blinding factors that commute with each other under the pairing. The main quality that characterize this paradigm is the greater flexibility provided by its algebraic structure. Since the identity presented in the Extract is in the form linear.

3.1.5 Selective Identity IBE/HIBE Security Notions

Selective Identity for an IBE function as follow, but we give only version CPA i.e without using the extraction decrypt queries in phase 1 :

Init :

The adversary outputs an identity ID^* where it wishes to be challenged.

Setup :

The challenger runs the Setup algorithm. It gives the adversary the resulting system parameters params. It keeps the master-key to itself.

Phase 1 :

The adversary issues queries q_1, \dots, q_m where query q_i is :

- Private key query $\langle ID_i \rangle$ where $ID_i \neq ID^*$ and ID_i is not a prefix of ID^* . The challenger responds by running algorithm KeyGen to generate the private key d_i corresponding to the public key $\langle ID_i \rangle$. It sends d_i to the adversary.

Challenge :

Once the adversary decides that Phase 1 is over it outputs two equal length plaintexts $M_0, M_1 \in \mathcal{M}$ on which it wishes to be challenged. The challenger picks a random bit $b \in \{0, 1\}$ and sets the challenge ciphertext to $C = \text{Encrypt}(\text{params}, ID^*, M_b)$. It sends C as the challenge to the adversary.

Phase 2 :

As phase 1

Guess :

Finally, the adversary outputs a guess $b_0 \in \{0, 1\}$. The adversary wins if $b = b_0$.

We refer to such an adversary A as an IND-sID-CPA adversary. We define the advantage of the adversary A in attacking the scheme E as $Adv_{\epsilon, A} = | \Pr[b = b_0] - \frac{1}{2} |$. The probability is over the random bits used by the challenger and the adversary.

We say that an IBE (or HIBE $ID = ID_1, ID_2, \dots, ID_k$ for a level k) system E is (t, q_{ID}, ϵ) -selective-identity, adaptive plaintext secure if for any IND-sID-CPA adversary A that runs in time t , makes at most q_{ID} chosen private-key queries, we have that $Adv_{\epsilon, A} = | \Pr[b = b_0] - \frac{1}{2} | < \epsilon$.

3.1.6 Selective⁺-ID Model

In Selective⁺-ID [14] we give a more power to the adversary. The power is a modification that will be given in the Challenge phase (prefix of the ID^*).

Challenge : A outputs two equal length messages M_0, M_1 and an identity $v+$ where $v+$ is either ID^* or any of its prefixes. In response it receives an encryption of M under $v+$, where v is chosen uniformly at random from $\{0, 1\}$. This model is more general than the sID model, because the adversary is allowed to ask for a challenge ciphertext not only on ID^* but also on any of its prefixes.

A protocol secure in the selective⁺-ID model is obviously secure in the selective-ID model.

3.1.7 Problem Bilinear of Diffie Hellman Assumption

During all the following section, we use the multiplicative expression instead of the additive one to simplify the proof of security. So we will give the following definition in the multiplicative expression.

Definition 8 :

((Decisional) Bilinear Diffie-Hellman Problem DBDHP). Let G_1, G_2 two rings with prime order q . Let

$\hat{e} : G_1 \times G_2 \rightarrow G_T$ be an application admissible and bilinear and let g be a generator of G_1 . The DBDHP in $\langle G_1, G_2, \hat{e} \rangle$ is so : Given $\langle g, g^a, g^b, g^c, z \rangle$ for $a, b, c \in \mathbb{Z}_q$ and $z \in G_2$. we say that an algorithm A that outputs $b \in \{0,1\}$ has advantage ε in solving the decision BDHP in G if :

$$| \Pr [g, g^a, g^b, g^c, \hat{e}(g, g)^{abc}] - \Pr [g, g^a, g^b, g^c, z] | > \varepsilon$$

where the probability is over the random choice of generator g in G_1 , the random choice of a, b, c in \mathbb{Z}_q , the random choice of $z \in G_2$, and the random bits of A . The distribution on the left is refereed as P_{BDHP} and the distribution on the right as R_{BDHP} .

Definition 9 :

((Decisional)k-Bilinear Diffie Hellman Inversion Problem (Dk-BDHIP)). Let k be an integer, and $x \in \mathbb{Z}_q^*, g \in G_2^*, \hat{e} : G_1 \times G_2 \rightarrow G_T, T \in G_T$. Can we make the following separation :

$$| \Pr [g, g^x, g^{x^2}, \dots, g^{x^k}, \hat{e}(g, g)^{\frac{1}{x}}] - \Pr [g, g^x, g^{x^2}, \dots, g^{x^k}, T] | > \varepsilon$$

Definition 10 :

((Decisional)k-Weak Bilinear Diffie Hellman Inversion Problem ($Dk - wBDHIP^*$)). Let k be an integer, and $x \in \mathbb{Z}_q^*, g \in G_2^*, \hat{e} : G_1 \times G_2 \rightarrow G_T, T \in G_T$. Can we make the following separation :

$$| \Pr [g, h, g^x, g^{x^2}, \dots, g^{x^k}, \hat{e}(g, h)^{x^{\frac{1}{x}}}] - \Pr [g, h, g^x, g^{x^2}, \dots, g^{x^k}, T] | > \varepsilon$$

3.2 Efficient IBE

Our second goal behind this work is to represent an efficient scheme in the model selective ID. This notion of security is weaker, Boneh et al prove that to pass from selective ID to full domain we will introduce a factor N . Additionally, as we have seen previously the BB1 is also more complex. We propose so to reduce this scheme or rather to propose a scheme in the approach Commutative Blinding and under the model Selective ID more reduced.

3.2.1 Construction

To avoid the use of two pairing in the Decrypt as with BB1, we collect in our approach the principal of the inverse in Extract as with BB2[4] and that's of the commutative Blinding[10], our procedure is as follow :

Our Scheme	
Setup. Let (G_1, G_T) a bilinear group. Choose a generator $g \in G_1$ and set $P_{pub_1} = g^l \in G_1^*$. Calculate $e(g, g) = x$ and $e(g, g)^a = x^a = y$. $M_{pk} = \{G_1, G_T, P_{pub_1}, x, y\}$. The Master secret key is $M_{sk} = \{1, a\}$ Message space is $\{0, 1\}^n$, ciphertext space is $G_1^* \times \{0, 1\}^n \times \{0, 1\}^n$.	
Extract : Given an identifier $ID_A \in \{0, 1\}^n$ of entity A, M_{pk} and M_{sk}	
Pick an $r_{ID_A} \in Z_q$, returns $g^{\frac{a+ID_A}{r_{ID_A}^t}} = g^{\frac{a}{r_{ID_A}^t} + r_{ID_A}^{t-1} ID_A} = g^{\frac{a' + r_{ID_A}^{t-1} ID_A}{t}}$, $d_A = (r_{ID_A}, g^{\frac{a+ID_A}{r_{ID_A}^t}})$	
Encrypt : Given a $m \in M$, ID_A and M_{pk} , the following step are formed :	
1. Pick a random s in Z_q	
2. Compute $z^{s(ID_A+a)} = e(g, g)^{s(ID_A+a)} = (x^{ID_A} y)^s$	
Set the ciphertext to be $C = (g^{ls} = P_{pub_1}^s, m, z^{s(ID_A+a)})$	
Decrypt : Given a ciphertext $C = (u, v) \in C$, ID_A , d_A and M_{pk} , follow the steps	
1. Compute $e(u^r, d_A)$ and output $m = \frac{v}{e(u^{r_{ID_A}}, g^{\frac{a+ID_A}{r_{ID_A}^t}})}$	

Firstly it is necessary to fix a security parameter t . l and follow the degree of security of this parameter.

Correctness

As we have :
 $e(u^{r_{ID_A}}, g^{\frac{a+ID_A}{r_{ID_A}^t}}) = e(g^{lsr_{ID_A}}, g^{\frac{a+ID_A}{r_{ID_A}^t}}) = e(g, g)^{s(ID_A+a)}$, our scheme is then correct

Observation

In our scheme we use the master key $(s, a, \hat{P} = \frac{1}{s} P_2)$, the private key will be $d_A = (r_{ID_A} (a + H_1(ID_A))) \hat{P}$. As a consequence the \hat{P} in our scheme will be computed one time and will be reuse to each demands, contrary to [4]. Noting that the syntax d_{A_1} of a given entity A_1 , we couldn't calculate the private key d_{A_2} for another entity A_2 , because we don't know a and we cannot inverse s . Also we change r_{ID_A} for each Identity.

3.2.2 Prove of Security

Before proving the security of our scheme, we note that k^- -BDHI, mean that we can use any $k > 0$ (it is not linked to the number of users as with [4]). And it is of our choice (we can choose it 2 or any number), by contrast with [4] we need at least 2^{50} (after [7]) for a 80 level of security.

The security of our scheme is basing on Dk^- -BDHI assumption since :

Theorem : Suppose the (t, k^-, ε) -Decision BDHI assumption holds in G of size $|G| = p$. Then our scheme is (t', q_S, ε) -selective identity, chosen plaintext (IND-sID-CPA) secure, with an advantage : $adv^{scheme}(t') > adv^{Dk^- - DBDHIP}(t - O(\tau q))$ for any $q_S < q$. Where τ is the time needed for an exponentiation in the following study.

Proof. Suppose A has advantage ε in attacking our scheme. We build an algorithm B that uses A to solve the Decision k^- -BDHI problem in G . Algorithm B is given as input a random $(k^- + 2)$ -tuple $(g, g^\alpha, g^{\alpha^2}, \dots, g^{\alpha^{k^-}}, T) \in G_1^{k^-+1} \times G_T$ that is either sampled from P_{BDHI} (where $T = e(g, g)^{1/\alpha}$) or from R_{BDHI} (where T is uniform and independent in G_T). The goal of the algorithm B is to output

1 if $T = e(g, g)^{1/\alpha}$ and 0 otherwise. Algorithm B works by interacting with A in a selective identity game as follows :

Setup.

To generate the system parameters, algorithm B does the following :

In the beginning algorithm A give B the identity $I^* = \frac{a_1}{b_1}$ that it intends to attack. The selective identity game begins, but algorithm B need to prepare to it the following step :

Preparation step

In the preparation step algorithm B choose an arbitrary x he compute $b_1 x$

After he compute (implicitly) : $f(\alpha) = \sum_{i=1}^{k^-} c_i \alpha^i$

He choose an arbitrary r_0 then he compute (implicitly) $r_1 = r_0 \sum_{i=1}^{k^-} c_i \alpha^{i-1}$

In the end he compute $h = g^{f(\alpha)}$ and he publish this h

Phase 1 :

A issues at most q_S private key queries, with $q_S < q$. Consider the i -th query for the private key corresponding to public key $ID_i \neq ID^*$.

We need to respond with a private key $(r, h^{\frac{a+r(I-I^*)}{\alpha}})$

The I represent a general identity ID and I^* represent an identity to be attacked

r is uniformly distributed in Z_p .

Algorithm B responds to the query as follows :

Firstly it is possible that the private key in our scheme may has the syntax $d_A = g^{\frac{a+ID_A}{t}}$ instead

of $d_A = g^{\frac{a+ID_A}{\tau t}} = g^{\frac{a}{\tau t}} + \frac{r' ID_A}{t} = g^{\frac{a' + r' ID_A}{t}}$. But we need this latter to simplify the proof

B pose $R = \frac{x}{r_0} + r_1$ he can calculate implicitly

$$\begin{aligned} R &= \frac{f(\alpha)}{f(\alpha)} \left(\frac{x}{r_0} + \frac{r_1}{I-I^*} (I - I^*) \right) \\ &= \frac{f(\alpha)}{\alpha \sum_{i=1}^{k^-} c_i \alpha^{i-1}} \left(\frac{x}{r_0} + \frac{r_1}{I-I^*} (I - I^*) \right) \\ &= \frac{f(\alpha)}{\alpha} \left(\frac{x}{r_0 \sum_{i=1}^{k^-} c_i \alpha^{i-1}} + \frac{r_1}{\sum_{i=1}^{k^-} c_i \alpha^{i-1} (I-I^*)} (I - I^*) \right) \\ &= \frac{f(\alpha)}{\alpha} \left(\frac{x}{r_0 \sum_{i=1}^{k^-} c_i \alpha^{i-1}} + \frac{r_0 \sum_{i=1}^{k^-} c_i \alpha^{i-1}}{\sum_{i=1}^{k^-} c_i \alpha^{i-1} (I-I^*)} (I - I^*) \right) \\ &= \frac{f(\alpha)}{\alpha} \left(\frac{x}{r_0 \sum_{i=1}^{k^-} c_i \alpha^{i-1}} + \frac{r_0}{I-I^*} (I - I^*) \right) \\ &= \frac{f(\alpha)}{\alpha} (a' + r' (I - I^*)) \end{aligned}$$

With $r' = \frac{r_0}{I-I^*}$ which is easy to calculate by B

But $a' = \frac{x}{r_0 \sum_{i=1}^{k^-} c_i \alpha^{i-1}}$ is not it is a Master key for B like α .

NB : (For the master key a , A can publish g^a in system of parameters. To remove this a , B search for an σ such that : $g^a g^\sigma = g^\alpha$)

So B can calculate easily g^R as he know $g^{\frac{x}{r_0}}$ and g^{r_0}

But $g^R = g^{\frac{f(\alpha)}{\alpha} (a' + r' (I - I^*))} = h^{\frac{a' + r' (I - I^*)}{\alpha}}$ which is a valid private key and so B can give A the private key $(r, h^{\frac{a' + r' (I - I^*)}{\alpha}})$

More B has not the advantage to calculate the private key for I^*

Challenge.

A outputs two messages $M_0, M_1 \in G_1$. Algorithm B picks a random bit $b \in \{0,1\}$ and a random $l' \in Z_p^*$. It responds with the ciphertext prepared as follow :

He have $h^s = h^{\frac{s}{\alpha} \cdot \alpha} = h^{l' \alpha} = c_1$, with $l' = \frac{s}{\alpha}$

And $c_2 = MT_h^{\frac{s(xb_1+a_1)}{b_1}} = T_h^{s(x+I^*)}$ (or rather $c_2 = MT_h^{\frac{s(ab_1+a_1)}{b_1}} = T_h^{s(a+I^*)}$)

So if $T_h = e(h, h)^{\frac{1}{\alpha}}$ he will have $e(h, h)^{\frac{s}{\alpha}(x+I^*)} = c_2 = e(h, h)^{l'(x+I^*)}$

And he combine $CT = (c_1, c_2) = (h^{l' \alpha}, e(h, h)^{l'(x+I^*)})$ which is a valid ciphertext under ID^*

If T_h is uniform in G_1 , then CT is independent of the bit b.

Phase 2.

A issues more private key queries, for a total of at most $q_S < q$. Algorithm B responds as before.

Guess.

Finally, A outputs a guess $b' \in \{0, 1\}$. If $b = b'$ then B outputs 1 meaning $T = e(g, g)^{\frac{1}{\alpha}}$. Otherwise, it outputs 0 meaning $T \neq e(g, g)^{\frac{1}{\alpha}}$.

When the input $k^- + 2$ -tuple is sampled from P_{BDHIP} (where $T = e(g, g)^{\frac{1}{\alpha}}$) then As view is identical to its view in a real attack game and therefore A must satisfy $|\Pr[b = b'] - 1/2| > \varepsilon$. On the other hand, when the input $k^- + 2$ -tuple is sampled from R_{BDHIP} (where T is uniform in G_T) then $\Pr[b = b'] = 1/2$. Therefore, with g uniform in G_1 , T uniform in G_T we have that :

$$\left| \Pr[g, g^\alpha, g^{\alpha^2}, \dots, g^{\alpha^{k^-}}, \hat{e}(g, g)^{\frac{1}{\alpha}}] - \Pr[g, g^\alpha, g^{\alpha^2}, \dots, g^{\alpha^{k^-}}, T] \right| \geq \left| \left(\frac{1}{2} \pm \varepsilon\right) - \frac{1}{2} \right| = \varepsilon.$$

Noting that in IBE, s^+ -ID and s-ID are the same, the difference may be in HIBE. □

3.2.3 Discussion

► Comparison with BB1 and BB2

In the following we compare the efficiency of our scheme with BB1 (version IBE[11] but under selective ID) and with BB2. We have seen above that we make a little change in BB2. This change is effective as we reduce the complexity of BB2. More than that our scheme is also more efficient than BB1(version IBE[11]). All this statements are summarized in table 6.

■ Compute of complexity

With the fact that :

For example $Expffi_{*/**}$: Exponentiation in the finite field involved in $*/**$, the * is the base of exponentiation, until the ** base of the exponent ; Pair : Pairing ; Inv : Inverse ; Mul : Multiplication.

As we have : $Complexity_{BB1} - Complexity_{Our} =$

$$\begin{aligned} & (3Pair + 1Divffi_{G_T/G_T} + 3Mulffi_{G_1/G_1} + 7Expffi_{G_1/Z_q} + 2Expffi_{G_T/Z_q}) - \\ & (2Pair + 1Divffi_{G_T/G_T} + 2Mulffi_{Z_q/Z_q} + 1Mulffi_{G_T/G_T} + 3Expffi_{G_1/Z_q} + 3Expffi_{G_T/Z_q} + 1Invffi_{Z_q/Z_q}) \\ & = \\ & 1Pair + 4Expffi_{G_1/Z_q} + 3Mulffi_{G_1/G_1} - 1Invffi_{Z_q/Z_q} - 2Mulffi_{Z_q/Z_q} - 1Mulffi_{G_T/G_T} - 1Expffi_{G_T/Z_q} >> 0 \end{aligned}$$

And we have : $Complexity_{BB2} - Complexity_{Our} =$

$$\begin{aligned} & (2Pair + 1Divffi_{G_T/G_T} + 2Mulffi_{G_1/G_1} + 1Expffi_{G_T/Z_q} + 7Expffi_{G_1/Z_q} + 1Invffi_{Z_q/Z_q} + 2Mulffi_{G_1/Z_q}) - \\ & (2Pair + 1Divffi_{G_T/G_T} + 2Mulffi_{Z_q/Z_q} + 1Mulffi_{G_T/G_T} + 3Expffi_{G_1/Z_q} + 3Expffi_{G_T/Z_q} + 1Invffi_{Z_q/Z_q}) \\ & = \\ & 4Expffi_{G_1/Z_q} + 1Mulffi_{G_1/G_1} + 2Mulffi_{G_1/Z_q} - 2Mulffi_{Z_q/Z_q} - 2Expffi_{G_T/Z_q} >> 0 \end{aligned}$$

Our scheme is then efficient than BB1 and BB2. Noting that in our scheme and BB2, we have taking into consideration the use of r which we need it only in the proof. The $\frac{1}{s}$ is calculate one time and we ruse its calculate for each demand.

TABLE 6 –

	BB1
Params	$2Exp_{ffi_{G_1/Z_q}} + 1Pair + 1Exp_{ffi_{G_T/Z_q}}$
Extract	$2Mul_{ffi_{Z_q/Z_q}} + 2Exp_{ffi_{G_1/Z_q}}$
Encrypt	$1Mul_{ffi_{Z_q/Z_q}} + 3Exp_{G_1/Z_q} + 1Exp_{ffi_{G_T/Z_q}}$
Decrypt	$2Pair + 1Div_{ffi_{G_T/G_T}}$
Sum	$3Pair + 1Div_{ffi_{G_T/G_T}} + 3Mul_{ffi_{G_1/G_1}} + 7Exp_{ffi_{G_1/Z_q}} + 2Exp_{ffi_{G_T/Z_q}}$
	BB2
Params	$2Exp_{ffi_{G_1/Z_q}} + 1Pair$
Extract	$1Mul_{ffi_{Z_q/Z_q}} + 1Inv_{ffi_{Z_q/Z_q}} + 1Exp_{ffi_{G_1/Z_q}}$
Encrypt	$1Mul_{ffi_{Z_q/Z_q}} + 3Exp_{ffi_{G_1/Z_q}} + 1Exp_{ffi_{G_T/Z_q}} + 1Mul_{ffi_{G_1/G_1}}$
Decrypt	$1Pair + 1Div_{ffi_{G_T/G_T}} + 1Mul_{ffi_{G_1/G_1}} + 1Exp_{ffi_{G_1/Z_q}}$
Sum	$2Pair + 1Div_{ffi_{G_T/G_T}} + 2Mul_{ffi_{G_1/G_1}} + 7Exp_{ffi_{G_1/Z_q}} + 1Inv_{ffi_{Z_q/Z_q}} + 2Mul_{ffi_{G_1/Z_q}}$
	Our
Params	$1Exp_{ffi_{G_1/Z_q}} + 1Pair + 1Exp_{ffi_{G_T/Z_q}}$
Extract	$1Exp_{ffi_{G_1/Z_q}} + 2Mul_{ffi_{Z_q/Z_q}} + 1Inv_{ffi_{Z_q/Z_q}}$
Encrypt	$1Mul_{ffi_{G_T/G_T}} + 2Exp_{ffi_{G_T/Z_q}} + 1Exp_{G_1/Z_q}$
Decrypt	$1Pair + 1Div_{ffi_{G_T/G_T}} + 1Exp_{ffi_{G_1/Z_q}}$
Sum	$2Pair + 1Div_{ffi_{G_T/G_T}} + 2Mul_{ffi_{Z_q/Z_q}} + 1Mul_{ffi_{G_T/G_T}} + 3Exp_{ffi_{G_1/Z_q}} + 3Exp_{ffi_{G_T/Z_q}} + 1Inv_{ffi_{Z_q/Z_q}}$

■ Concrete Comparison : Technique of Boyen

Using the technique (or rather the base) of Boyen [11], we obtain so the following result. But, to balance the comparison between the scheme, we consider that BB1 functions with symmetric pairing as our scheme and BB2.

SS @ 80-bit security level

	BB1	BB2	Our
Extract :	4	2	2
Encrypt :	108	108	106
Decrypt :	320	222	222
Sum	432	332	330

MNT @ 80-bit security level

	BB1	BB2	Our
Extract :	0,4	0,2	0,2
Encrypt :	100,8	100,8	100,6
Decrypt :	320	220,2	220,2
Sum	421,2	321,2	321

SS : Curve Supersingular

MNT : Curve MNT

So according to these result, our scheme is more efficient than BB1. It's complexity is nearest to BB2, but we will confirms that our scheme is efficient than BB2. As this latter is basing in its study of simulation in Dk-BDHIP, with k is linked to the request identity. By contrast, our scheme is basing in Dk⁻-BDHIP, k⁻ < k. So our scheme is more efficient than BB2 according to the result of Cheon[20].

3.3 Efficient HIBE

3.3.1 Our Construction

As we have cited above, Boneh ,Boyen and Goh [17] have proposed an efficient scheme. This scheme reduce the ciphertext of an HIBE from k parameters to a shorten one of only three parameters. And the Decrypt from k product of pairing, to only two pairing. But [17] necessitate that the use of the identity to be chosen will be taken in Z_q^* which limit the selection of the identity, more than that [17] doesn't support the selective⁺ID. In the following proposition we overcome all this weakness.

Our Scheme	
Setup.	Let (G_1, G_T) a bilinear group. Choose a generator $g \in G_1$ and set $P_{pub_1} = g^l \in G_1^*$. Calculate $e(g, g) = x$ and $e(g, g)^{a_1} = x^{a_1} = y_1, e(g, g)^{a_2} = x^{a_2} = y_2, \dots, e(g, g)^{a_v} = x^{a_v} = y_v$. (or rather $g^{a_1}, g^{a_2}, \dots, g^{a_v}$). $M_{pk} = \{G_1, G_T, P_{pub_1}, x, y_1, g^{a_1}, y_2, g^{a_2}, \dots, y_v, g^{a_v}\}$, $M_{sk} = \{1, a_i / 1 \leq i \leq v\}$ Message space is $\{0, 1\}^n$, ciphertext space is $G_1^* \times \{0, 1\}^n \times \{0, 1\}^n$.
Extract :	Given an identifier $ID_A = (I_{A_1}, \dots, I_{A_j}) \in Z_p^j$ of depth $j \leq v$, of an entity A, public key M_{pk} , master key M_{sk} returns For a depth j, we have $d_A = g^{\frac{a_1 + I_{A_1} + a_2 + I_{A_2} + \dots + a_j + I_{A_j}}{l}}$ The private key is $(g^{\frac{a_1 + I_{A_1} + a_2 + I_{A_2} + \dots + a_j + I_{A_j}}{l}}, g^{\frac{1}{l}}, g^{\frac{a_{j+1}}{l}}, \dots, g^{\frac{a_v}{l}})$ (or $(e(g, g)^{\frac{a_1 + I_{A_1} + a_2 + I_{A_2} + \dots + a_j + I_{A_j}}{l}}, e(g, g)^{\frac{1}{l}}, e(g, g)^{\frac{a_{j+1}}{l}}, \dots, e(g, g)^{\frac{a_v}{l}})$) Noting that for level j+1, choose $s_{j+1} \in Z_p$ and calculate $(g^{\frac{a_1 + I_{A_1} + a_2 + I_{A_2} + \dots + a_j + I_{A_j} + s_{j+1}(a_{j+1}) + I_{A_{j+1}}}{l}}, g^{\frac{1}{l}}, g^{\frac{a_{j+2}}{l}}, \dots, g^{\frac{a_v}{l}})$
Encrypt :	Given $m \in M$, ID_A and M_{pk} , the following step are formed : 1. pick a random s in Z_q 2. Compute $z^{s(I_{A_1} + a_1 + I_{A_2} + a_2 + \dots + I_{A_j} + a_j)} = e(g, g)^{s(I_{A_1} + a_1 + I_{A_2} + a_2 + \dots + I_{A_j} + a_j)} = (x^{I_{A_1} + I_{A_2} + \dots + I_{A_j}} y_1 y_2 \dots y_j)^s$ Ciphertext is $C = (g^l = P_{pub_1}^s, g^s, m, z^{s(I_{A_1} + a_1 + I_{A_2} + a_2 + \dots + I_{A_j} + a_j)})$
Decrypt :	Given $C = (u', u'', v') \in C, ID_A, d_A, M_{pk}$, follow the step 1. Compute $e(u', d_A)$ and output $m = \frac{v' e(u'', g^{(s_j-1)a_j})}{e(u', d_A)}$

Observation

- ★ The private key $(g^{\frac{a_1 + I_{A_1} + a_2 + I_{A_2} + \dots + s_j(a_j) + I_{A_j}}{l}}, g^{\frac{1}{l}}, g^{\frac{a_{j+1}}{l}}, \dots, g^{\frac{a_v}{l}}) = (d_0, d_1, \dots, d_{v-1})$ is a private key for the Entity in Hierarchy (Children). For the user the private key will be $(d_0, g^{(s_j-1)a_j})$, if we are in a level j.
- ★ l and $a_j, j \in \{1, \dots, v\}$ follow a certain level of security. What is mean that they are belonging in 2^t for a parameter t of security chosen in beginning (following for example the requirement of NIST)

3.3.2 Prove of Security

The security of our scheme is basing on $DL - BDHI_{WC}$ (which mean DL-BDHI With Condition, in the following the condition is $g^{\alpha^l} = 1$) assumption since :

Theorem : Suppose the (t, l, ε) -Decision $BDHI_{wc}$ assumption holds in G . Then our scheme is (t', q_S, ε') -selective identity, chosen plaintext (IND-sID-CPA) secure such that :

$Adv^{scheme}(t', q_S, \varepsilon') \geq Adv^{l-BDHI_{WC}}(t, l, \varepsilon)$ where $t' > t - O(\log \tau)$. Where τ is the time needed to make an exponentiation in the following proof :

Proof. Suppose A has advantage in attacking our scheme. We build an algorithm B that uses A to solve the Decision $l - BDHI_{WC}$ problem in G . Algorithm B is given as input a random $(l+3)$ -tuple $(g, g^\alpha, g^{\alpha^2}, \dots, g^{\alpha^{l-1}}, l, T) \in G_1^* \times Z_q \times G_T$ such that $g^{\alpha^l} = 1$, this input is either sampled from P_{BDHI} (where $T = e(g, g)^{\frac{1}{\alpha}}$) or from R_{BDHI} (where T is uniform and independent in G_T). The goal of the algorithm B is to output 1 if $T = e(g, g)^{\frac{1}{\alpha}}$ and 0 otherwise. Algorithm B works by interacting with A in a selective identity game as follows :

Initialization.

We note for the selective identity $ID^* = (I_1^*, \dots, I_k^*) \in (Z_p)^k$ which algorithm A intends to attack. If $k < v$, B concatenate by 1 to have exactly v (the depth of the hierarchy).

Setup.

As algorithm A can give to B the $(g, g^\alpha, g^{\alpha^2}, \dots, g^{\alpha^l}, 1 / g^{\alpha^l} = 1)$ according to its choice. So depending on the identity $ID^* = (I_1^*, \dots, I_k^*)$ chosen. A choose an arbitrary j from $[1, k]$, for example $j=2$. He calculate $(g^{-I_2^*}, g^{-I_2^* \alpha}, g^{-I_2^* \alpha^2}, \dots, g^{-I_2^* \alpha^l}, 1 / g^{\alpha^l} = 1)$. Implicitly he calculate : $f(\alpha) = \sum_{i=0}^s \alpha^i$, $t(\alpha) = f(\alpha) - f(0)$, also $\frac{t(\alpha)}{\alpha} = \frac{f(\alpha) - f(0)}{\alpha} = f'(\alpha)$. s will be chosen according to some requirement in phase 1.

Our goal is to test if B can output the private key

$d_A = (h^{\frac{a_1 + a_2 + \dots + a_k + I_1 - I_1^* + I_2 - I_2^* + \dots + I_k - I_k^*}{\alpha}}, h^{\frac{1}{\alpha}}, h^{\frac{a_{k+1}}{\alpha}}, h^{\frac{a_{k+2}}{\alpha}}, \dots, h^{\frac{a_v}{\alpha}}) = (d_0, d_1, d_3, \dots, d_{v-2})$ for a given v and an identity (I_1, \dots, I_v)

B first picks a random $\gamma_1, \gamma_1, \dots, \gamma_v \in Z_p^*$ which will verify some conditions in phase 1

Phase 1.

A issues up to q_S private key queries.

In the first step, choose an identity $ID = (I_1, \dots, I_r)$, such that $r \leq v$

If $r \leq k$, he selections only r element from ID^* and if $r \geq k$ the adversary B concatenate k (the depth of I^*) by 1 as we have seen above.

To response to d_0 , B can make the following step :

B imagine (implicitly) that each a_i ($1 \leq i \leq v$) can be writ as $a_i = \gamma_i + (-1)^i \alpha^i$ (*)

Noting that B can make this, as he can choose a suitable γ_i such that $g^{\alpha^i} = g^{a_i} g^{\gamma_i}$. We privilege to use the syntax (*), because $f(\alpha) g^{\alpha^i}$ can be not calculate-see the following

So $\frac{f(\alpha) - f(0)}{\alpha} \sum_{i=1}^{i=k} a_i = \frac{f(\alpha) - f(0)}{\alpha} \sum_{i=1}^{i=k} (\gamma_i + (-1)^i \alpha^i) = f'(\alpha) \sum_{i=1}^{i=k} \gamma_i \cdot f'(\alpha) \sum_{i=1}^{i=k} (-1)^i \alpha^i$

The first part $f'(\alpha) \sum_{i=1}^{i=k} \gamma_i$ can be calculate easily (after exponent it by g), until the second may not. But if we regroup it, we can find that $f'(\alpha) \sum_{i=1}^{i=k} (-1)^i \alpha^i =$

$$\sum_{i=1}^{i=s} \alpha^{i-1} (-\alpha + \alpha^2 - \alpha^3 + \dots + \alpha^{k-1} + \alpha^k) \\ = - \sum_{i=1}^{i=s} \alpha^i + \sum_{i=1}^{i=s} \alpha^{i+1} - \sum_{i=1}^{i=s} \alpha^{i+2} + \dots + (-1)^{k-1} \sum_{i=1}^{i=s} \alpha^{i+k-2} + (-1)^k \sum_{i=1}^{i=s} \alpha^{i+k-1}.$$

To remove the overstepping α , B must choose its s such that $s+k-1=l$ i.e $s=l-k-1$ which imply that the most long factor : α^{i+s-1} is equal to 1. Thus B can calculate easily

$$g^{\frac{f(\alpha) - f(0)}{\alpha} (-I_2^*) \sum_{i=1}^{i=k} a_i} = h^{\frac{\sum_{i=1}^{i=k} a_i}{\alpha}}, \text{ (with } h = g^{(f(\alpha) - f(0))(-I_2^*)} = g^{f''(\alpha)(-I_2^*)} \text{) which is equal to} \\ g^{(f'(\alpha) \sum_{i=1}^{i=k} \gamma_i) (- \sum_{i=1}^{i=s} \alpha^i + \sum_{i=1}^{i=s} \alpha^{i+1} - \sum_{i=1}^{i=s} \alpha^{i+2} + \dots + (-1)^{k-1} \sum_{i=1}^{i=s} \alpha^{i+k-2} + (-1)^k \sum_{i=1}^{i=s} \alpha^{i+k-1}) (-I_2^*)} =$$

$$g(f'(\alpha) \sum_{i=1}^{i=k} \gamma_i)(-\alpha - \alpha^3 - \dots (-1)^k \alpha^{s+k-1})(-I_2^*).$$

For the second part : $R = h^{\frac{I_1 - I_1^* + I_2 - I_2^* + \dots + I_k - I_k^*}{\alpha}}$. To output the exact key of ID at which all elements of ID operate in d_0 , all the I_i chosen will be different from I_2^* . And to benefit from $f''(\alpha)$, all I_i (for all $1 \leq i \leq r$) of the requested identity ID, will be such that : $I_i \neq nI_2^*$ from each to other and this for $n \in N$. Because he wouldn't obtain $f''(\alpha)$, but he may obtain another $f'''(\alpha)$.

Observation

A can choose $(g^{-I_k^*}, g^{-I_2^* \alpha^2}, g^{-I_4^* \alpha^4}, \dots, g^{-I_{k-1}^* \alpha^{k-1}}, 1 / g^{\alpha^l} = 1)$ instead of $(g^{-I_2^*}, g^{-I_2^* \alpha^2}, \dots, g^{-I_2^* \alpha^l}, 1 / g^{\alpha^l} = 1)$ (we treat this later i.e only with I_2^* to simplify the proof). So if B make a research exhaustive to know the exact place of I_i^* for $1 \leq i \leq v$, he need at most doing v research, which cost $(v!)$, as v can be great. So for all $1 \leq i \leq v$ the $I_i \neq nI_2^* \forall n \in N$. And this is an ideal case.

To calculate R , B will calculate firstly d_1 . And to do it, B can calculate $\frac{f(\alpha) - f(0)}{\alpha} = f'(\alpha)$.

After he calculate $g^{\frac{f(\alpha) - f(0)}{-\alpha}(-I_2^*)} = g^{\frac{f''(\alpha)(-I_2^*)}{\alpha}} = g^{f'(\alpha)(-I_2^*)} = h^{\frac{1}{\alpha}} = d_1$. With this, B can calculate easily R , as he exponents only with $I_1 - I_1^* + I_2 - I_2^* + \dots + I_k - I_k^*$.

Now to calculate d_3, d_4, \dots, d_{v-2} , we have respectively the coefficients $\alpha, \alpha^2, \alpha^3, \dots, \alpha^{s+v-1}$ after a product of a_{k+1}, \dots, a_v with $f'(\alpha)$. Effectively, all j overstepping l i.e $l=j-x$ their $\alpha^j = \alpha^x$, with $x < l$ \square

Thus with this manner B can responds to the private key

$$d_A = (h^{\frac{a_1 + a_2 + \dots + a_k}{\alpha} + \frac{I_1 - I_1^* + I_2 - I_2^* + \dots + I_k - I_k^*}{\alpha}}, h^{\frac{1}{\alpha}}, h^{\frac{a_{k+1}}{\alpha}}, h^{\frac{a_{k+2}}{\alpha}}, \dots, h^{\frac{a_v}{\alpha}})$$

Challenge.

A outputs two messages $M_0, M_1 \in G_1$. Algorithm B picks a random bit $b \in \{0,1\}$ and a random $l' \in Z_p^*$. It responds with the ciphertext prepared as follow :

He have $g^{(f(\alpha) - f(0))(-I_2^*)^s} = h^{\frac{s}{\alpha} \alpha} = h^{l' \alpha} = c_1$, with $l' = \frac{s}{\alpha}$

And $c_2 = MT_h^{s(a_1 + a_2 + \dots + a_k + I_1^* + I_2^* + \dots + I_k^*)} = T_h^{s(a_1 + a_2 + \dots + a_k + I_1^* + I_2^* + \dots + I_k^*)}$

So if $T_h = e(h, h)^{\frac{1}{\alpha}}$ he will have

$$e(h, h)^{\frac{s}{\alpha}(a_1 + a_2 + \dots + a_k + I_1^* + I_2^* + \dots + I_k^*)} = c_2 = e(h, h)^{l'(a_1 + a_2 + \dots + a_k + I_1^* + I_2^* + \dots + I_k^*)}$$

And he combine CT = $(c_1, c_2) = (h^{l' \alpha}, e(h, h)^{l'(a_1 + a_2 + \dots + a_k + I_1^* + I_2^* + \dots + I_k^*)})$ which is a valid ciphertext under ID^*

If T_h is uniform in G_1 , then CT is independent of the bit b .

Phase 2.

A issues more private key queries, for a total of at most $q_S < q$. Algorithm B responds as before.

Guess.

Finally, A outputs a guess $b' \in \{0, 1\}$. If $b = b'$ then B outputs 1 meaning $T = e(g, g)^{\frac{1}{\alpha}}$.

Otherwise, it outputs 0 meaning $T \neq e(g, g)^{\frac{1}{\alpha}}$.

When the input $l + 2$ -tuple is sampled from P_{BDHIP} (where $T = e(g, g)^{\frac{1}{\alpha}}$) then As view is identical to its view in a real attack game and therefore A must satisfy $|\Pr[b = b'] - 1/2| > \varepsilon$. On the other hand, when the input $l + 2$ -tuple is sampled from R_{BDHIP} (where T is uniform in G_T) then $\Pr[b = b'] = 1/2$. Therefore, with g uniform in G_1 , T uniform in G_T we have that :

$$\left| \Pr [g, g^\alpha, g^{\alpha^2}, \dots, g^{\alpha^{l-1}}, 1, \hat{e}(g, g)^{\frac{1}{\alpha}}] - \Pr [g, g^\alpha, g^{\alpha^2}, \dots, g^{\alpha^l}, 1, T] \right| \geq \left| \left(\frac{1}{2} \pm \varepsilon \right) - \frac{1}{2} \right| = \varepsilon \quad \square$$

3.3.3 Discussion

Our first discussion will be about the problem used in the proof, which is $Dl - BDHI_{WC}$. We have considers in the above that $l \gg v$ (v is the depth of the hierarchy). But, this can make our proposition vulnerable to the cryptanalysis of Cheon [20] by comparison with $Dl - wBDHI^*$ in [17]. As in this latter, $l \leq v$ (v the depth of the hierarchy), since in the [20] cheon prove that the strong Diffie-Hellman problem has a complexity reduction $O(\sqrt{l})$ by comparison with PDL. So while k is great, while it will be easy to be cryptanalysis. To avoid this, we propose to consider $l=v+l'$, we can use so $\alpha' = \beta$ instead of α to reduce the problem from $Dl - BDHI_{WC}$ to $Dv - BDHI_{WC}$ and even we can make less of this.

We note that the relationship between the problem used is :

$l - BHIP \xrightarrow{1} l - wBDHI^* \xrightarrow{2} l - BDHI_{WC}$ (so :

$Dl - BHIP \xrightarrow{1} Dl - wBDHI^* \xrightarrow{2} Dl - BDHI_{WC}$). The relation 1 was proven in [17], until 2 is easy to be proven.

Even if [17], is basing on a strong problem of Diffie Hellman compared to our (this may be linked to the use of asymmetric pairing). But [17] has two weakness, which are the obliged use of the selection identity in the study of simulation in Z_p^* instead of Z_p as with our. This limit the selection of the identity to be challenged, since we couldn't use any were the bit 0. More than that the [17] does not support $s^+ID - CPA$, by contrast our scheme is like BB1 support this notion. According to [14] to render [17] $s^+ID - CPA$, the authors make a simple modification. Its proof yields a multiplicative security degradation by a factor of v , where v is the maximum number of levels in the HIBE. And to not obtain this degradation the authors add $v-k$ factors or rather $(v-k)Exp_{G_1}$ in the original scheme (v is the maximum depth of the Hierarchies, until k is the depth of the identity selected ID^*)

By contrast with our scheme we don't need this, because our scheme is $s^+ID - CPA$ and it offer a competitive to [17]

To see this we count in the following the complexity of BB1, BBG, and our scheme :

	$Extract_{user}$ level k	Encrypt	Decrypt
BB1	$(2k+3)Exp_{G_1}$	$(2k+1)Exp_{G_1} + 1Exp_{G_T}$	$(k+1)pairing + kMul_{G_T}$
BBG	$3Exp_{G_1}$	$(k+2)Exp_{G_1} + 1Exp_{G_T}$	$2pairing$
Our	$2Exp_{G_1}$ or $2Exp_{G_T}$	$(k+2)Exp_{G_T} + 2Exp_{G_1}$	$2 pairing + 1Mul_{G_T} + 1Exp_{G_1}$

In this table we wouldn't take into account some complexity (like division of pairing, multiplicity by $y_1y_2...y_k$ in our scheme, multiplicity by g_3 in BBG...)

According to this table our scheme is more efficient by comparison with BB1 and with even BBG. Because, Exp_{G_T} which we count it as $Exp_{Z_{p^{k'}}$ (in the finite field) is small than Exp_{G_1} (i.e in curve elliptic).

This efficient is visible in Extract, and Encrypt (for the two scheme BB1 and BBG). For the Decrypt we have a little overstepping by comparison with BBG, but because of what we seen in the highest (in the point of view security), our scheme is so more efficient.

3.4 Application

3.4.1 Overview on Forward Encryption

In [13] Canetti et al propose a forward-secure encryption scheme in the standard model basing on [16]. The (fs-HIBE) scheme allows each user in the hierarchy to refresh his or her private keys periodically while keeping the public key the same. Using this, so even if there are any were a compromise of long-term keys it does not permit the compromise of the past session keys and therefore past communications. Since exposure of a secret key corresponding to a given interval

does not enable an adversary to break the system for any prior time period. For more detail, we send the interested to [13][33].

To admit a succeed Forward Security, the following requirements will be realizing :

- New users would be able to join the hierarchy and receive secret keys from their parent nodes at any time.
- The encryption does not require knowledge of when a user or any of his ancestors joined the hierarchy, we call this joining-time-oblivious. So the sender can encrypt the message as long as he knows the current time and the ID-tuple of the receiver, along with the public parameters of the system.
- The scheme should be forward-secure.
- Refreshing secret keys can be carried out autonomously, that is, users can refresh their secret keys on their own to avoid any communication overhead with any PKG.

Eventually jointing [13] and [16] can give a scheme which can not verify these requirements. For more detail see [33]. To over come this the authors in [33], have proposed a scheme (basing in [13]) which conserve all these requirements, but they use only HIBE of [16], which give a heavy scheme. In the following we give a version at which we use our syntax of an HIBE (we declared it only). This reduce the complexity, but because of some circumstance, we wouldn't give in this article it's proof of security. We let it, in the future work and to the interested.

Implementation : Declaration

Firstly we note $sk_{w,(ID_1,...,ID_v)}$: a node key associated with some prefix w of he bit representation of a time period i and a tuple $(ID_1, ..., ID_v)$.

$SK_{i,(ID_1,...,ID_v)}$: Key associated with time i and an ID-tuple $(ID_1, ..., ID_v)$. It consists of sk keys as follows : $SK_{i,(ID_1,...,ID_v)} = \{sk_{i,(ID_1,...,ID_v)}, sk_{w1,(ID_1,...,ID_v)} : w0 \text{ is a prefix of } i\}$. With W0 and W1 represent respectively node right and node left.

Setup($1^k, N = 2^l$)

The root PKG with ID_1 does the following :

1. IG is run to generate groups G_1, G_T of order q and bilinear map \hat{e} .
 2. A random generator g of G_1 is selected
 3. $P_{pub1} = g^l \in G_1^*$.
 4. Calculate $e(g, g) = x$, $e(g, g)^{a_1} = x^{a_1} = y_1$, $e(g, g)^{a_2} = x^{a_2} = y_2, ..., e(g, g)^{a_v} = x^{a_v} = y_v$.
(or rather $g^{a_1}, g^{a_2}, ..., g^{a_v}$).
- $M_{pk} = \{G_1, G_T, P_{pub1}, x, y_1, g^{a_1}, y_2, g^{a_2}, ..., y_v, g^{a_v}\}$, $M_{sk} = \{1, a_i / 1 \leq i \leq v\}$

The following algorithm is a helper method, it is called by the Setup and Upd algorithms.

CompNext($sk_{w,h}, w, (ID_1...ID_v)$)

It takes a secret key $sk_{w,v}$, a node w , and an ID-tuple, and outputs keys $sk_{(w0),v}, sk_{(w1),v}$ for time nodes $w0$ and $w1$ of $(ID_1...ID_v)$.

1. Parse w as $w_1...w_d$, where $|w| = d$. Parse ID-tuple as $ID_1, ..., ID_v$. Parse $sk_{w,h}$ associated with time node w , for all $1 \leq k \leq d$ and $1 \leq j \leq v$.
2. Choose random $s_{(d+1),j} \in Z_q$ for all $1 \leq j \leq h$.
3. Set $S_{(w0),v} =$

$$(g^{\frac{a_{d+1,1} + w0 \circ I_{A_1} + a_{d+1,2} + w0 \circ I_{A_2} + ... + a_{d+1,j-1} + w0 \circ I_{A_{j-1}} + s_{d+1,j}(a_{d+1,j}) + w0 \circ I_{A_j}}{l}}, g^{\frac{1}{l}}, g^{\frac{a_{d+1,j+1}}{l}}, ..., g^{\frac{a_{d+1,v}}{l}})$$

$$S_{(w1),h} = \left(g^{\frac{a_{d+1,1}+w1 \circ I_{A_1} + a_{d+1,2}+w1 \circ I_{A_2} + \dots + a_{d+1,j-1}+w1 \circ I_{A_{j-1}} + s_{d+1,j}(a_{d+1,j})+w1 \circ I_{A_j}}{l}}, g^{\frac{1}{l}}, g^{\frac{a_{d+1,j+1}}{l}}, \dots, g^{\frac{a_{d+1,v}}{l}} \right)$$

4. Erase $s_{(d+1),j}$ for all $1 \leq j \leq v$.

KeyDer($SK_{i,(v-1)}, i, (ID_1 \dots ID_v)$)

Let E_h be an entity that joins the hierarchy during the time period $i < N - 1$ with ID-tuple (ID_1, \dots, ID_v) . E_h 's parent generates E_v 's key $SK_{i,v}$ using its key $SK_{i,(v-1)}$ as follows :

1. Parse i as $i_1 \dots i_l$ where $l = \log_2 N$. Parse $SK_{i,(v-1)}$ as $(sk_{i,(v-1)}, \{sk_{(i|_{k-1}1),(v-1)}\}_{i_k=0})$.
2. For each value $sk_{w,(v-1)}$ in $SK_{i,(v-1)}$, E_v 's parent does the following to generate E_h 's key $sk_{w,v}$: (a) Parse w as $w_1 \dots w_d$, where $d \leq l$, and parse the secret key $sk_{w,(v-1)}$ as $(S_{w,(v-1)}, g^{\frac{1}{l}}, g^{\frac{a_{w,v}}{l}})$.
(b) Choose random $s_{k,v} \in Z_q$ for all $1 \leq k \leq d$. Recall that $s_{k,j}$ is a shorthand for $s_{w|_k, (ID_1 \dots ID_j)}$ associated with time node $w|_k$ and tuple $(ID_1 \dots ID_j)$.
(c) Set the child entity E_v 's secret point $S_{w,v}$

$$= g^{\frac{a_{1,1}+w|_k \circ I_{A_1} + a_{2,2}+w|_k \circ I_{A_2} + \dots + a_{j-1,j-1}+w|_k \circ I_{A_{j-1}} + s_{d+1,j}(a_{j,j})+w|_k \circ I_{A_j}}{l}}.$$

E_h 's parent sets $SK_{i,h} = (sk_{i,h}, \{sk_{(i|_{k-1}1),h}\}_{i_k=0})$, and erases all other information.

Upd($SK_{i,h}, i+1, (ID_1 \dots ID_v)$) (where $i < N - 1$)

At the end of time i , an entity (PKG or individual) with ID-tuple (ID_1, \dots, ID_v) does the following to compute its private key for time $i+1$, as in the fs-PKE scheme [].

1. Parse i as $i_1 \dots i_l$, where $|i| = l$. Parse $SK_{i,v}$ as $(sk_{(i|_l),v}, \{sk_{(i|_{k-1}1),v}\}_{i_k=0})$. Erase $sk_{i|_l,h}$.
2. We distinguish two cases. If $i_l = 0$, simply output the remaining keys as the key $SK_{(i+1),v}$ for the next period for ID-tuple (ID_1, \dots, ID_h) . Otherwise, let \tilde{k} be the largest value such that $i_{\tilde{k}} = 0$ (such \tilde{k} must exist since $i < N - 1$). Let $i' = i|_{\tilde{k}-1}1$. Using $sk_{i',h}$ (which is included as part of $SK_{i,v}$), recursively apply algorithmCompNext to generate keys $sk_{(i'0^d1),v}$ for all $0 \leq d \leq l - \tilde{k} - 1$, and $sk_{(i'0^{d-\tilde{k}},v)}$. The key $sk_{(i'0^{d-\tilde{k}},v)}$ will be used for decryption in the next time period $i+1$, the rest of sk keys are for computing future keys. Erase $sk_{i',v}$ and output the remaining keys as $SK_{(i+1),v}$.

Enc($i, (ID_1, \dots, ID_v), M$) (where $M \in \{0, 1\}^n$)

1. Parse i as $i_1 \dots i_l$
2. Denote $P_{k,j} = H_1(i|_k \circ ID_1 \dots ID_j)$ for all $1 \leq k \leq l$ and $1 \leq j \leq h$.
3. pick a random s in Z_q
4. Compute $z^{s(a_{|2,1}+i|_2 \circ ID_1 + \dots + a_{|j,1}+i|_j \circ ID_1 + a_{|1,1}+i|_1 \circ ID_1 + \dots + a_{|1,j}+i|_1 \circ ID_1 \dots ID_j + \dots + a_{|j,1}+i|_j \circ ID_1 + \dots + a_{|j,j}+i|_j \circ ID_1 \dots ID_j)} = e(g, g)^{s(a_{|2,1}+i|_2 \circ ID_1 + \dots + a_{|j,1}+i|_j \circ ID_1 + a_{|1,1}+i|_1 \circ ID_1 + \dots + a_{|1,j}+i|_1 \circ ID_1 \dots ID_j + \dots + a_{|j,1}+i|_j \circ ID_1 + \dots + a_{|j,j}+i|_j \circ ID_1 \dots ID_j)}$
Ciphertext is $C = (g^s = P_{pub_1}^s, g^s, m.z^{s(a_{|2,1}+i|_2 \circ ID_1 + \dots + a_{|j,1}+i|_j \circ ID_1 + a_{|1,1}+i|_1 \circ ID_1 + \dots + a_{|1,j}+i|_1 \circ ID_1 \dots ID_j + \dots + a_{|j,1}+i|_j \circ ID_1 + \dots + a_{|j,j}+i|_j \circ ID_1 \dots ID_j)})$

Decrypt : Given $C = (u', u'', v') \in C, ID_A, d_A, M_{pk}$, follow the step

1. Parse i as $i_1 \dots i_l$. Parse $SK_{i,h}$ associated with the ID-tuple as $(sk_{i,h}, \{sk_{(i|_{k-1}1),h}\}_{i_k=0})$.
2. Compute $e(u', d_A)$ and output $m = \frac{v' e(g^s, g^{s a_{|j,1} + \dots + a_{|j,j}})}{e(u', d_A)}$

Comparison

To see the efficiency of our scheme (and BBG) in forward scheme we make the following comparison.

	fs-HIBE [33]	fs-with our
Key derivation time	$O(v \log N)$	$O((v-k) \log N)$
Encryption time	$O(v \log N)$	$O(v \log N)$
Decryption time	$O(v \log N)$	$O(k + \log N)$
Key update time	$O(v)$	$O(v-k)$
Ciphertext length	$O(v \log N)$	$O(3 \log N)$
Public key size	$O(v + \log N)$	$O(v + \log N)$
Secret key size	$O(v \log N)$	$O((v-k) \log N)$

k is the hierarchy children considered.

N is the total number of the time periods.

v is depth of the hierarchy.

3.5 Construction of CCA2

This section is reserved to signal the technique to be used to obtain a CCA2 from CPA.

To render CPA a CCA2, there are some techniques :

For an IBE or HIBE with random oracle we can use the two method given by Fujusiki Okamoto [34]

For an IBE or HIBE without random oracle, there are also two techniques :

That's of [13] at which we use one-time signature.

That's of [35] at which we add a MAC.

So using one of these last technique can render our scheme CCA2 secure.

4 Conclusion

In these papers, we have study the competition between the best-known cryptosystems of the cryptography IBE. Our approach is more accurate than the only method made in this direction of Boyen. Even if we follow a very simple strategy but it is so effective to clarify the cryptosystems that deserve a standardized participation. We concluded that the pattern of Boneh and Franklin in the field of RO, is the most effective, but we recommend using one of Skai Kasarah since Boneh and Franklin projects into an elliptic curve which limit the selection of curve, it may so pose a problems of security. And we note that unlike the results of Boyen the BB1 is late compared to others. In general we can say that the scheme of Water is the most preferable as it is traced in the domain of SM, more it has an important classification. Following the criteria considered SK and BF are the most helpful.

This study is very useful to cryptographers, because we surveying the very recents recherches in IBE. More we shows the weakness and strength of every cryptosystem in competition, which can facilitate to make an improvement to admit a more practical cryptosystems.

More than that, we have presented two efficient schemes in the model selective ID and without random oracle (which is our second contribution behind this work). With a little change in the schemes of Boneh and Boyen we get a more efficient schemes. The change is make in BB2 (change $\frac{1}{s+ID}$ by $\frac{1}{s}$), which permit to eliminate the use of two pairing in the Decrypt of IBE and, more the resulting scheme is traced in the approach of commutative Blinding. Effectively as it is presented in this article, the complexity of our scheme is less than that of BB1 (version IBE) and even than

that of BB2. More than that, we have based our prove of security in Dk^- -BDHIP which is an efficient problem than Dk -BDHIP used by BB2, since with this latter, k is linked essentially to the numbers of identity to be challenged. By contrast, with our we are not, any k^- can serve us, we can take as title of example $k^-=2$, which make Dk^- -BDHIP in competition with DBDHP (D1-BDHIP) used by BB1. In other part, using our syntax of IBE in HIBE and using the technique of BBG (Boneh Boyen Goh) we get a more efficient HIBE than BB1 and BBG. The efficiency by comparison with BB1, is clearly seen in complexity. With our proposition, the technique of BBG will be more efficient. Because, with our proposition the complexity will be reduced. More than that, our HIBE support s^+ -ID (which require a degradation by v in the studies of simulations) and we can not demand that the identity to be challenged will be in Z_q^* as with BBG. This render BBG more restricted, as we are are not free to choose the identity to be challenged. Using our proposition in some applications like Forward Encryption make them more efficient.

Thus, during all these papers, we have presented an efficient IBE and HIBE without random oracle. With a little change in BB2 we obtain an efficient schemes than BB1 and BB2, which are considered until 2011 (Journal of Cryptology) as the most efficient schemes in the model selective ID and without random oracle.

Acknowledge

We would like to thank the head of our laboratory Mr.Aboutajdinne Driss.

Références

- [1] A. Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology - CRYPTO'84*, volume 196 of *Lecture Notes in Computer Science*, pages 47-53. Springer-Verlag, 1985.
- [2] D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3) :586-615, 2003.
- [3] D. Boneh and X. Boyen. Efficient selective-ID secure identity based encryption without random oracles. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004*, volume 3027, pages 223-238, 2004.
- [4] R. Sakai and M. Kasahara. ID based cryptosystems with pairing on elliptic curve. *Cryptology ePrint Archive*, Report 2003/054.
- [5] B. Waters. Efficient identity-based encryption without random oracles. In Ronald Cramer, editor, *Advances in Cryptology - EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 114-127. Springer-Verlag, 2005.
- [6] Gentry. Practical identity-based encryption without random oracles. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 445-464. Springer-Verlag, 2006.
- [7] E. Kiltz, Y. Vahlis. CCA2 Secure IBE : Standard Model Efficiency through Authenticated Symmetric Encryption. *CT-RSA 08*, *Lecture Notes in Computer Science Vol. ,* T. Malkin ed., Springer-Verlag, 2008.
- [8] E. Kiltz. Chosen-ciphertext secure identity-based encryption in the standard model with short ciphertexts. *Cryptology ePrint Archive*, Report 2006/122, 2006.

- [9] IEEE P1363.3 Committee. IEEE 1363.3 - standard for identity-based cryptographic techniques using pairings. <http://grouper.ieee.org/groups/1363/>, April 2007.
- [10] X. Boyen. The BB1 identity-based cryptosystem : A standard for encryption and key encapsulation. Submitted to IEEE 1363.3, aug 2006. <http://grouper.ieee.org/groups/1363/>.
- [11] X. Boyen. A tapestry of identity-based encryption : Practical frameworks compared. *International Journal of Applied Cryptography*, 1(1) :3-21, 2008.
- [12] M. Bellare, A. Desai, D. Pointcheval, and Ph Rogaway. Relations among notions of security for public-key encryption schemes, volume 1462 *Lecture Notes in Computer Science*, pages 26-45. Springer-Verlag, 1998
- [13] R. Canetti, S. Halevi, and J. Katz. Chosen-ciphertext security from identity-based encryption. In *Advances in CryptologyEUROCRYPT*, volume 3027 of *LNCS*, pages 20722. Springer-Verlag.
- [14] Sanjit Chatterjee and Palash Sarkar. Constant Size Ciphertext HIBE in the Augmented Selective-ID Model and its Extensions. *IACR eprint archive report 084/2007*.
- [15] J. Horwitz and B. Lynn. Toward hierarchical identity-based encryption. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 466-481. Springer-Verlag, 2002.
- [16] C. Gentry and A. Silverberg. Hierarchical ID-based cryptography. In Yuliang Zheng, editor, *Advances in Cryptology - ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 548-566. Springer-Verlag, 2002.
- [17] D. Boneh, X. Boyen, and Eu-Jin Goh. Hierarchical identity based encryption with constant size ciphertext. In Ronald Cramer, editor, *Advances in Cryptology - EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 440-456. Springer-Verlag, 2005.
- [18] D. Boneh and X. Boyen. Efficient selective-ID secure identity based encryption without random oracles. *Journal of Cryptology (JOC)*, 24 (4) :659-693, 2011. Extended abstract in proceedings of Eurocrypt 2004, *LNCS 3027*, pp. 223-238, 2004 i.e [5]
- [19] L. Chen, Zh. Cheng || Security Proof of Sakai-Kasahara’s Identity-Based Encryption Scheme || In *Proceedings of Cryptography and Coding 2005*.
- [20] J. Cheon. Security analysis of the strong Diffie-Hellman problem. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 1-11. Springer-Verlag, Berlin, Germany, May / June 2006.
- [21] M. Bellare and P. Rogaway. Random oracles are practical : a paradigm for designing efficient protocols. In *Proceedings of the First Annual Conference on Computer and Communications Security*, ACM, 1993.
- [22] Gaëtan Leurent and Phong Q. Nguyen. How risky is the random-oracle model ? In Halevi [18], pages 445-464.
- [23] D. Galindo. A separation between selective and full-identity security notions for identity-based encryption Available on : *IACR eprint archive*.
- [24] L. Martin. "Introduction To Identity Based Encryption". Available at : <http://www.artechhouse.com/GetBlob.aspx?strName=Martin-238-CH04.pdf>
- [25] D. Galindo || Boneh-Franklin identity based encryption revisited ||. In *Proceedings of the 32nd International Colloquium on Automata, ICALP 2005*.
- [26] S. Galbraith, K. Paterson, and N. Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, 156(16) :3113-3121, 2008.

- [27] S. Marie-Aude « Etude de la Primalité motivée par le besoin de Nombres Premiers dans le Chiffrement RSA » sur le site : <http://www-magistere.u-strasbg.fr/IMG/pdf/MASteineur.pdf>
- [28] H.Cohen, G. Frey. Handbook of Elliptic and Hyperelliptic Curve Cryptography.
- [29] Tetsuya Izu and Tsuyoshi Takagi. Efficient Computations of the Tate Pairing for the Large MOV Degrees. In ICISC 2002, volume 2587 of Lecture Notes in Computer Science, pages 283-297. Springer Verlag, 2003.
- [30] Nadia El Mrabet, Arithmétique des couplages, performance et résistance aux attaques par canaux cachés. December 2009, Thèse.
- [31] N. Koblitz and A. Menezes. Pairing-based cryptography at high security levels. In Nigel P. Smart, editor, Cryptography and Coding, volume 3796 of Lecture Notes in Computer Science, pages 13-36, Berlin, Heidelberg, 2005. Springer-Verlag.
- [32] Galindo and Ichiro Hasuo. Security Notions for Identity Based Encryption. available on : <http://eprint.iacr.org/2005/253>
- [33] D.(Daphne) YAO, N.FAZIO , Y.DODIS and A.LYSYANSKAYA. Forward-Secure Hierarchical IBE with Applications to Broadcast Encryption. Chapter of book : Identity-Based Cryptography, in M. Joye and G. Neven (Editors). 2009.
- [34] E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Proceedings of Advances in Cryptology - CRYPTO '99, LNCS 1666, pp. 535-554, Springer-Verlag, 1999.
- [35] D. Boneh and J. Katz. Improved efficiency for CCA-secure cryptosystems built using identity based encryption. Submitted for publication, 2004.